Internet-Draft
Expires: March, 2002

Yoshihiro Ohba, Editor
Nobuyasu Nakajima
Toshiba America Research, Inc.

Tao Zhang
Telcordia Technologies

September 12, 2001

LH-DMHA - Last Hop DMHA (Dormant Mode Host Alerting) Protocol

<draft-ohba-seamoby-last-hop-dmha-02.txt>

Status of This Memo

Key Words

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.

Abstract

This document specifies a protocol for alerting a dormant mode host of incoming packets. A unique characteristic of the proposed protocol is that its major operations, namely, paging registration, monitoring and capturing of paging triggering packets, and initiation of the paging operation, are performed primarily in a last-hop subnet (i.e., the edge subnet to which the host is connected before entering

dormant mode). The proposed protocol conforms with the DMHA (Dormant Mode Host Alerting) protocol requirements discussed in the IETF Seamoby WG.

Table of Contents

1. Terminology

The following terminology is defined in this document.

Host (H)

A standard IP host in the sense of STD0003, with an additional capability to enter dormant mode.

Last Hop Subnet (LHS)

The edge subnet to which a Host is connected. We use the word "Last Hop Subnet" instead of "Edge Subnet", because the main purpose of protocol is alerting a dormant mode host of "incoming" packets.

Last Hop (LH)

The final hop for a packet to reach a Host on the Last Hop Subnet.

Paging Area

Collection of radio access points that are signaled to locate a dormant mode Host. In this specification, paging area is defined in the sense of L3 paging and thus it is also referred to as "L3 paging area". An L3 paging area can be configured independently of L2 technologies or L2 paging areas, even on top of L2 technologies that do not have L2 paging. The mapping between an L3 paging area and L2 paging area is entirely an implementation issue and thus out of scope of this document.

A dormant mode Host may be required to signal to the network when it crosses a paging area boundary, in order that the network can maintain a rough idea of where the Host is located.

An arbitrary mapping between subnets and paging areas is allowed in this protocol.

Tracking Agent (TA)

A node that is responsible for tracking a Host's location while it is in dormant mode. Each Host is served by a single Tracking Agent. Multiple Tracking Agents can exist in an administrative domain in a way that each Tracking Agent keeps track of an

exclusive set of Hosts.

Paging Agent (PA)

A node that is responsible for alerting a dormant Host when there is an incoming packet for the Host. Additionally, the Paging Agent

maintains Paging Areas by periodically wide casting information over the Host's link to identify the Paging Area. The paging area information may be wide cast at L2 or it may also involve IP. Each paging area is served by a unique set of Paging Agents.

Note that it is described in the requirements document [DMHA-REQ] that each paging area is served by a unique functional element "Paging Agent". In this specification, the Paging Agent functionality is realized by using one or more protocol entities of the same name "Paging Agent".

Dormant Monitoring Agent (DMA)

A router in the sense of RFC1812, which locates in a last hop subnet and detects the delivery of packets to a Host that is in Dormant Mode (and thus does not have an active L2 connection to the Internet). It is the responsibility of the Dormant Monitoring Agent to inform the Paging Agent to page the Host via a Tracking Agent. Until the Host wakes up with establishing a routable connection to the Internet, the Dormant Monitoring Agent buffers the packet destined for the Host.

A Dormant Monitoring Agent can be co-located with Mobile IP Home Agent or Foreign Agent to realize Home Agent Paging or Foreign Agent Paging introduced in [RAMJEE2001]. A Dormant Monitoring Agent can be separated from Home Agent or Foreign Agent, which can be viewed as a realization of a special case of Domain Paging [RAMJEE2001].

Agent

An Agent is one of a Dormant Monitoring Agent, a Tracking Agent or a Paging Agent.

Session

An aggregate state maintained between peering Agents.

2. Protocol Overview

LH-DMHA is an application layer protocol which runs over UDP. LH-DMHA consists of four basic operations: paging registration, paging area update, paging, and paging deregistration. Each operation is illustrated in Figures 1, 2, 3 and 4, respectively.

When a Host which is in active mode decides to enter a dormant mode, it performs paging registration with the Dormant Monitoring Agent on the last hop subnet to which it is currently connecting. If the IP address of the Dormant Monitoring Agent is previously unknown, it multicasts a DMA Solicitation message on the last hop subnet and the Dormant Monitoring Agent replies with a DMA Advertisement message. DMA Advertisement message is also periodically multicast on the last

hop subnet. Once the IP address of the Dormant Monitoring Agent is known, the Host sends a DMA Registration message to the Dormant Monitoring Agent, specifying the lifetime of the registration. Then, the Dormant Monitoring Agent registers the information specified in the received message and returns a DMA Registration ACK message to the Host. If paging area update operation is supported by a Tracking Agent, the Dormant Monitoring Agent also sends a TA Registration message to the Tracking Agent on behalf of the Host and waits for a TA Registration ACK message before returning a DMA Registration ACK message. When the Host finally receives the DMA Registration ACK message, it is able to enter dormant mode.

After entering dormant mode, the Host may detect a paging area change. Then, the Host MAY perform paging area update operation. There are three methods for paging area update operation. If the L2 supports paging area registration mechanism, the Host MAY perform L2 paging area update, which MAY result in sending a TA Registration message from a Paging Agent to the Tracking Agent to update the location of the Host (U1, U2 and U3 in Figure 2). Alternatively, the Host MAY send a TA Registration message directly to the Tracking Agent (U1' and U2' in Figure 2). Or the Host MAY perform paging registration with the Dormant Monitoring Agent that has been taking care of the dormant Host, with specifying the updated paging area information, and as a consequence, the Dormant Monitoring Agent sends a TA Registration message to the Tracking Agent (not illustrated in Figure 2).

The Dormant Monitoring Agent monitors packets on the subnet, and when it captures a packet that is worth awaking the registered dormant Host, it performs paging operation by sending a Paging message to a set of Paging Agents via Tracking Agent. The Paging message is delivered to the Tracking Agent by using unicast. The Tracking Agent forwards the Paging message to Paging Agents by using either unicast or multicast. When a Paging Agent receives a Paging message, it performs an action to awake the dormant Host. If L2 supports paging, the L2 paging SHOULD be involved in the action. The Paging message MAY be delivered to the dormant Host in a way that is receivable by the Host. Alternatively, if the Dormant Monitoring Agent is aware of the exact location of the Host, it MAY directly deliver the paging trigger packet to the dormant Host. If the Paging message is delivered to the dormant Host, the Host MUST authenticate the message. The Dormant Monitoring Agent SHOULD buffer the captured packet until the Host performs paging deregistration operation or a paging timeout timer expires.

When the Host exits a dormant mode either spontaneously due to e.g., originating a SIP call or starting web-browsing or passively as a result of receiving a Paging message, a paging trigger packet or an

L2 paging message, it performs paging deregistration operation by sending a DMA Registration message to the Dormant Monitoring Agent with which the Host has been registering, with specifying a lifetime of zero, and then receiving a corresponding DMA Registration ACK message from the DMA.

Paging area information is advertised by Paging Agents on either traffic channel or signaling channel or both. When paging area information is advertised on traffic channel, it is carried in Paging

Area Advertisement messages periodically multicast.

All messages defined in this specification except for DMA Solicitation and DMA Advertisement messages MUST be authenticated. See sections "LH-DMHA Security Model", "LH-DMHA Authentication" and "Security Consideration" for details.

If any of two Agents or all Agents are co-located in a single node, it is not needed to carry LH-DMHA messages exchanged between those Agents over UDP or authenticate the messages. Any mechanism can be used for exchanging information between those Agents.

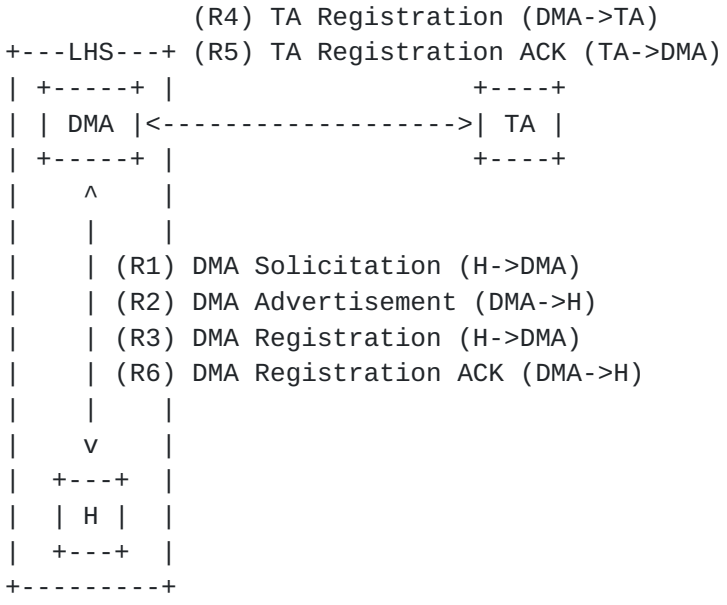


Figure 1: LH-DMHA registration operation

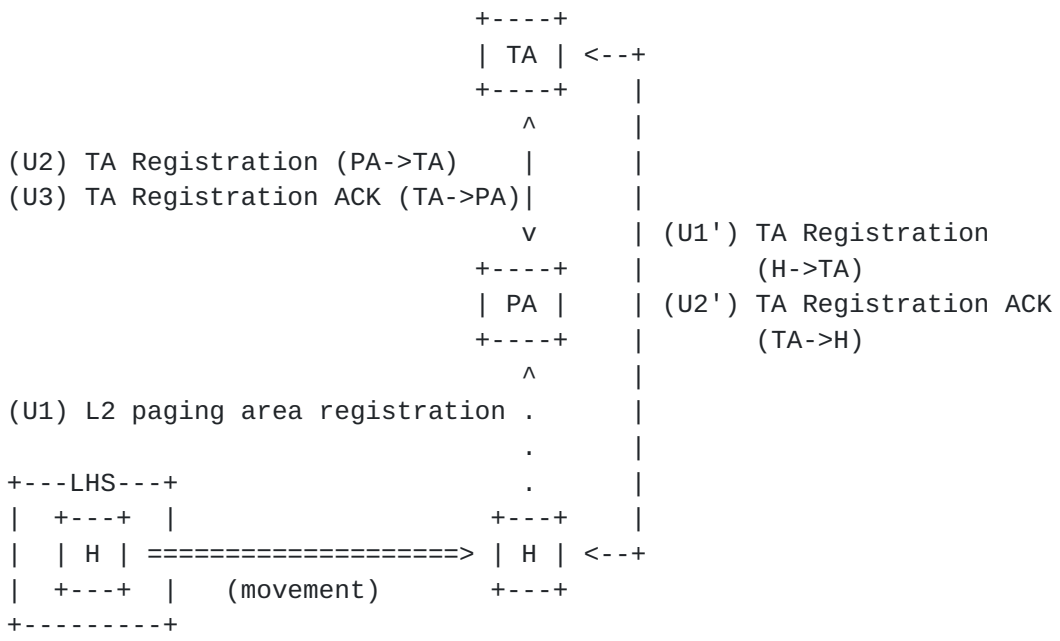


Figure 2: LH-DMHA paging area update operation

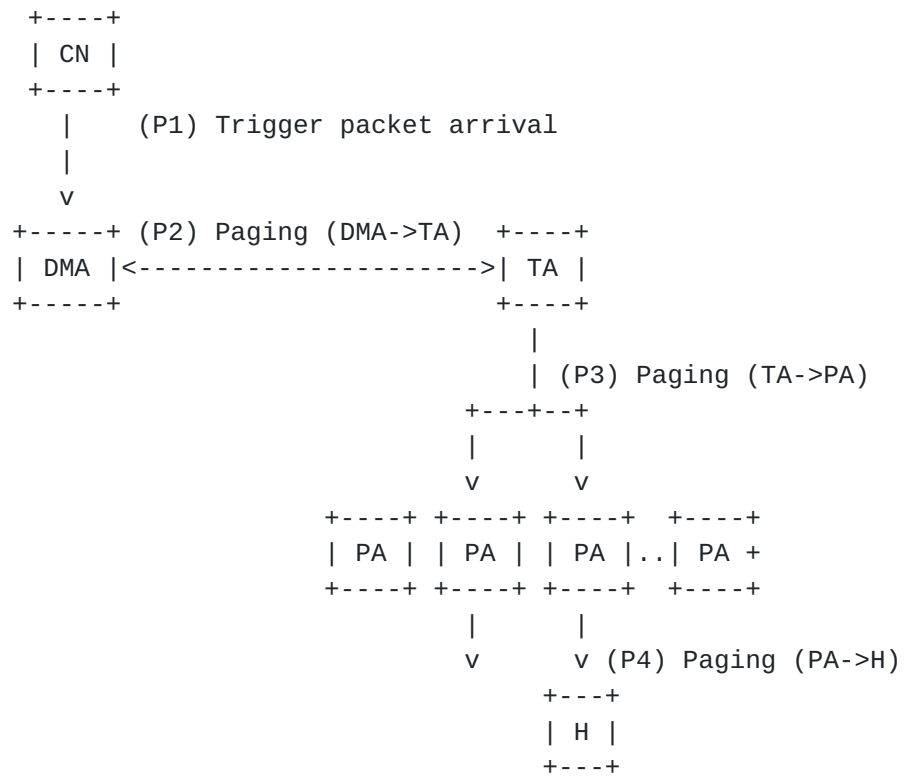


Figure 3: LH-DMHA paging operation

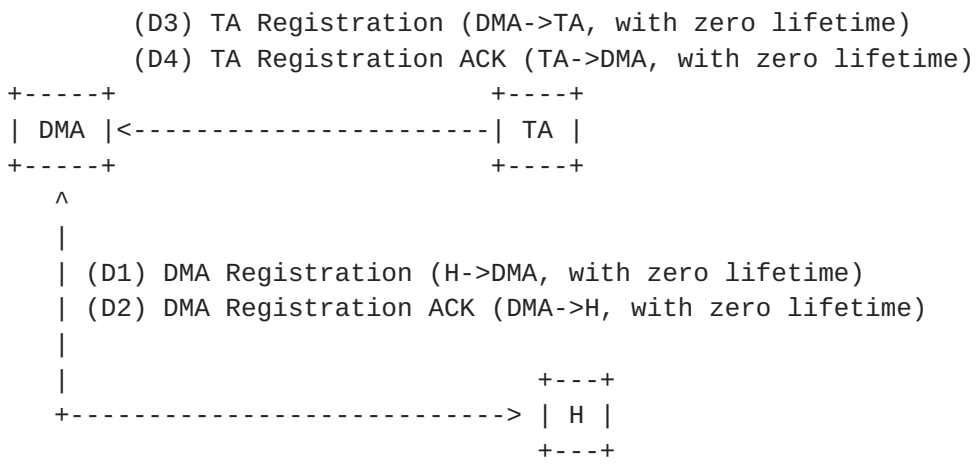


Figure 4: LH-DMHA deregistration operation

3. LH-DMHA Security Model

LH-DMHA defines its own built-in authentication mechanism, called LH-DMHA authentication, which is used for authenticating LH-DMHA messages.

All the LH-DMHA messages exchanged directly or indirectly between the protocol entities except for DMA Solicitation and DMA Advertisement message MUST be authenticated by using the LH-DMHA authentication. The Security Association (SA) which is used for LH-DMHA authentication is referred to as a DMHA-SA. See Figure 5 for the LH-DMHA security model.

LH-DMHA does not provide a mechanism to establish the DMHA-SA. Instead, a number of methods could be used such as IKE, URP and statically shared key.

The DMHA-SA used for authenticating Paging Area Advertisement messages is a special SA for which the same shared secret MAY be shared among all Hosts and all Paging Agents. Such sharing is as a result of consideration of tradeoff between the security impact of bogus paging area advertisement and difficulty for establishing an SA between Paging Agents and a specific Host.

Although LH-DMHA does not have a mechanism to encrypt LH-DMHA messages, it is possible to use IPsec ESP for message encryption, provided that an IPsec SA can be established between entities.

See sections "Security Consideration" and "LH-DMHA Authentication" for details.

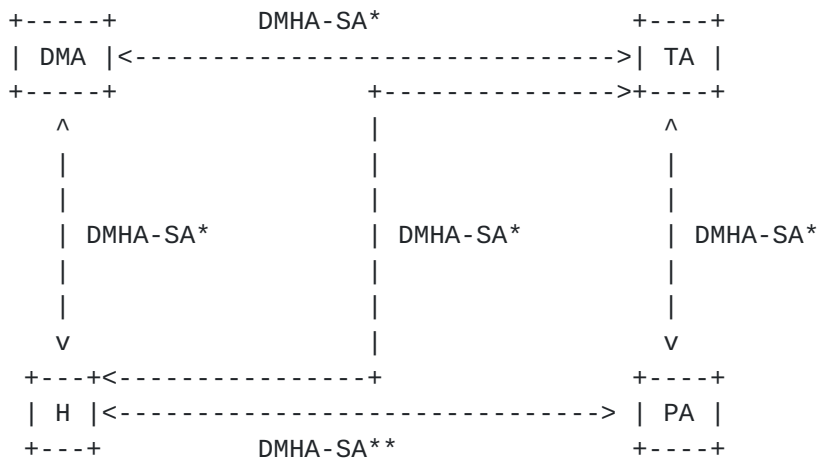


Figure 5: LH-DMHA Security Model

4. Protocol Description

4.1. Transport

The LH-DMHA uses UDP as its transport. The UDP port number is TBD.

4.2. DMA Discovery

If a Host does not know the IP address of the Dormant Monitoring Agent, it multicasts DMA Solicitation message on the last hop subnet. A Host MAY also send a DMA Solicitation message whenever it wakes up from dormant mode, which MAY be used for detecting a subnet change.

The multicast address for IPv4 DMA Solicitation is TBD.

The multicast address for IPv6 DMA Solicitation is TBD.

When a Dormant Monitoring Agent receives a DMA Solicitation message from a Host, it returns a DMA Advertisement message to the Host. In addition, a Dormant Monitoring Agent periodically sends a DMA Advertisement message on the last hop subnet. Solicited DMA Advertisement messages are unicast to the sender of the DMA Solicitation message. Unsolicited DMA Advertisement messages are multicast on the last hop subnet. The scope of the multicast MUST be limited within the last hop subnet.

The multicast address for IPv4 DMA Advertisement is TBD.

The multicast address for IPv6 DMA Advertisement is TBD.

DMA Solicitation messages and DMA Advertisement messages are not authenticated.

/* Authors' note : It is also possible to utilize ICMP Router Solicitation and Router Advertisement for the purpose of DMA Discovery. */

4.3. Advertising Paging Area Information

If paging area information is advertised from the network, it is advertised by Paging Agents on either traffic channel or signaling channel or both. When paging area information is advertised on traffic channel, it is carried in Paging Area Advertisement messages periodically multicast by Dormant Monitoring Agents.

When paging area information is advertised on signaling channel, it MAY be carried in Paging Area Advertisement messages if the signaling channel supports carrying IP packets, or it MAY be carried by using L2 specific method which is not specified in this document.

The multicast address for IPv4 Paging Area Advertisement is TBD.

The multicast address for IPv6 Paging Area Advertisement is TBD.

4.4. Capability Set

A DMA Advertisement message contains a set of capabilities that is supported by the network. The following capability set is defined in this version of specification. Each capability can be specified independently.

- Implicit paging registration: If this capability is supported, a Host does not need to explicitly perform paging registration operation before it enters dormant mode. Implicit paging registration is useful when the Host and Dormant Monitoring Agent is connected on a point-point link. Implicit paging registration is also useful when the Dormant Monitoring Agent is co-located with an access point which is able to know both the dormant state and the mapping between the hardware address and IP address(es) of the Host.

- Non-mandatory paging area update: If this capability is supported, a Host can continue to be dormant when it crosses a paging area boundary. In other words, Host does not have to perform paging area update operation each time it crosses a paging area boundary. Furthermore, if this capability is supported, a Host does not even have to perform paging area update operation at all. The specific methods used by a Host to determine when to perform paging update operation is up to the implementation of specific location update and paging algorithms.

- TA Registration from Paging Agent: If this capability is supported, Paging Agents automatically perform paging area update operation on behalf of a Host when the Host perform L2 paging area registration.

- TA Registration from Host: If this capability is supported, a Host is allowed to send a TA Registration message to a Tracking Agent to perform paging area update operation.

- Paging trigger packets specified by Host: If this capability is supported, a Host is allowed to specify the set of paging trigger packets in a DMA Registration message.

- o Optimization for mobility management protocol: If this capability is supported, the Dormant Monitoring Agent advertising this capability is co-located with a Mobility Agent (e.g., a Home Agent in Mobile IP or Mobile IPv6 or a Foreign Agent in Mobile IP) and a Host is exempt from performing periodical mobility binding after successful paging registration.

4.5. Paging Registration

Before a Host enters dormant mode, it sends a DMA Registration message to the Dormant Monitoring Agent and waits for a DMA Registration ACK message. A DMA Registration message contains the hardware address of the interface of the Host that is going to be dormant and the lifetime of the registration. The lifetime used for paging registration MUST be greater than zero.

The Dormant Monitoring Agent then registers the specified information in the received Registration message and returns a DMA Registration ACK message to the Host. The DMA Registration ACK message contains a result of paging registration operation and the lifetime. The lifetime contained in the DMA Registration ACK message can be different from that is specified by the Host if the specified value is out of the range that is supported by the Dormant Monitoring Agent. If paging area update operation is supported by a Tracking Agent, the Dormant Monitoring Agent also sends a TA Registration message to the Tracking Agent on behalf of the Host and waits for a TA Registration ACK message before returning a DMA Registration ACK message. Finally, when the Host receives a DMA Registration ACK message for the DMA Registration message from the Dormant Monitoring Agent with a result indicating successful registration, it is able to enter a dormant mode.

To refresh the paging registration state, the registered Host sends a DMA Registration message to the Dormant Monitoring Agent before the next lifetime expires.

The Host SHOULD retransmit the DMA Registration message until a corresponding DMA Registration ACK message is received from the Dormant Monitoring Agent.

Note that if the Dormant Monitoring Agent supports implicit paging registration, a Host can enter dormant mode without sending DMA Registration messages.

If ARP or Neighbor Discovery is used in the last hop subnet, the following consideration is needed.

- The Dormant Monitoring Agent MUST NOT delete its ARP/Neighbor cache entry for the dormant Host while the Host is registered.

- If a Host is not able to receive broadcast frames in dormant mode, it SHOULD delete all the ARP/Neighbor cache entries while it is in dormant mode, as those entries will not be updated and thus will

become obsolete.

4.6. Paging Area Update

After entering dormant mode, the Host may detect paging area change based on the paging area information advertised on traffic channel or signaling channel (see Section "Advertising Paging Area Information"). Then, the Host MAY perform paging area update operation in the following way.

If L2 supports paging area registration mechanism, and the network supports TA Registration from Paging Agent described in section "Capability Set", the Host MAY perform L2 paging area update, which MAY result in sending a TA Registration message from a Paging Agent to the Tracking Agent to update the location of the Host.

Alternatively, if the network supports TA Registration from Host described in section "Capability Set", the Host MAY send a TA Registration message directly to the Tracking Agent. In this case, if the network supports the capability of "non-mandatory paging area update" described in section "Capability Set", the Host MAY enter dormant mode without waiting for a TA Registration ACK message from the Tracking Agent. In this case, A-flag is set to be zero in the header of the TA Registration message. See section "Message Format" for the usage of A-flag.

Alternatively, the Host MAY perform paging registration with the Dormant Monitoring Agent that has been registering the dormant Host, with specifying the updated paging area information, and as a consequence, the Dormant Monitoring Agent sends a TA Registration message to the Tracking Agent.

In the last two cases, the Host would need to configure a new IP address before sending the TA Registration message without deleting the old IP address so that it can receive a TA Registration ACK message from the Tracking Agent as well as Paging messages from the Dormant Monitoring Agent regarding the old IP address.

4.7. Monitoring Paging Trigger Packets

A Dormant Monitoring Agent monitors the subnet to which the Hosts are connected in order to capture paging trigger packets. Currently the following set of paging trigger packets is defined by default:

o Any unicast IP packet in which the destination IP address matches

the IP address of a registered dormant Host.

- Broadcast ARP REQUEST message in which the target network layer address matches the IP address of a registered dormant Host.

- In IPv6 case, Neighbor Solicitation message to the target dormant

Host. The destination address of this message is either the solicited-node multicast address which corresponds to the target dormant Host, or the IPv6 address of the target dormant Host.

If the Host performs paging registration with specifying a set of trigger packets in a DMA Registration message, the specified set of trigger packets overrides the default set of trigger packets. For example, a Host MAY specify a set of trigger packets so that it is awaken only when a SIP message destined for the Host is received at the Dormant Monitoring Agent.

If the Dormant Monitoring Agent is connected to the last hop subnet only, and thus is not acting as a gateway to the Internet, the Dormant Monitoring Agent SHOULD perform proxy- and gratuitous- ARP or Neighbor Advertisement on behalf of the dormant Host in order to capture paging trigger packets.

A Dormant Monitoring Agent MAY filter out paging trigger packets originated from a specific set of correspondent nodes for security purposes.

/* Authors' note : There is a discussion on the seamoby mailing list on defining a new ICMP error code used for informing correspondent nodes of the dormant status of the Host. */

4.8. Paging

When a Dormant Monitoring Agent captures a paging trigger packet, it sends a Paging message to the Tracking Agent. The Tracking Agent then determines a set of Paging Agents to forward the Paging message and forwards it to the Paging Agents. The forwarding is performed by either unicast or multicast.

When a Paging Agent receives a Paging message, it performs an action to awake the dormant Host. If L2 supports paging, the L2 paging SHOULD be involved in the action. The Paging message MAY be delivered to the dormant Host in a way that is receivable by the Host. Alternatively, if the Dormant Monitoring Agent is aware of the exact location of the Host, it MAY directly deliver the paging trigger packet to the dormant Host. If the Paging message is delivered to the dormant Host, the Host MUST authenticate the message.

The Dormant Monitoring Agent SHOULD buffer the captured packet and retransmit the Paging message until the Host performs paging deregistration operation or a paging timeout timer expires. The Paging message is not acknowledged hop-by-hop. Instead, the paging

deregistration attempt by the Host (e.g., arrival of a DMA Registration message with a lifetime of zero) is used as the end-to-end acknowledgment for the Paging message. So the Dormant Monitoring Agent SHOULD retransmit the Paging message until a DMA Registration message with a lifetime of zero is received from the Host or a paging timeout timer expires.

4.9. Detecting Inactive Hosts

A dormant Host may become inactive without performing paging deregistration for some reasons, such as bad radio conditions or battery exhaustion. In such a situation, consideration is needed for not increasing traffic used for paging the Host. To this end, the Dormant Monitoring Agent considers that the Host becomes inactive when a paging timeout timer expires. While the Host is considered to be inactive, the Dormant Monitoring Agent MUST delay the next paging operation for a while and MUST NOT buffer paging trigger packets during the delay. The interval between successive paging operations SHOULD be increased exponentially while the Host is considered to be inactive.

4.10. Paging Deregistration

When a Host exits a dormant mode either spontaneously due to e.g., originating a SIP call or starting web-browsing or passively as a result of receiving a Paging message, it sends a DMA Registration message to the Dormant Monitoring Agent with specifying the lifetime of zero. The Dormant Monitoring Agent then removes the entry for the Host from its database and returns a DMA Registration ACK message to the Host with specifying the lifetime of zero. The Dormant Monitoring Agent also sends a TA Registration message to the Host with specifying the lifetime of zero and the Tracking Agent returns a TA Registration ACK with specifying the lifetime of zero to the Dormant Monitoring Agent.

Alternatively, the Host MAY perform paging registration with a new Dormant Monitoring Agent of the new last hop subnet where it exits a dormant mode in order to enter a dormant mode again. In this case, the Host MAY not need to perform paging deregistration operation with the old Dormant Monitoring Agent. Instead, the Tracking Agent MAY perform paging deregistration with the old Dormant Monitoring Agent on behalf of the Host when it receives TA Registration message from the new Dormant Monitoring Agent. If this happens, the Tracking Aegnt sends a DMA Registration message to the old Dormant Monitoring Agent with specifying a lifetime of zero and waits for a DMA Registration ACK message from the Dormant Monitoring Agent.

If the Host runs a mobility management protocol, then mobility binding update MUST be performed when it enters the active mode in order to re-establish a routable L3 link with the Internet.

Note that the Host can enter the active mode before it receives a DMA Registration ACK message for paging deregistration, or even before it sends a DMA Registration message for paging deregistration.

4.11. Configuring Paging Areas

Paging area identifiers to be advertised from a Paging Agent are configured either manually or automatically at the Paging Agent.

When paging area identifiers are configured automatically, a Tracking Agent sends a Paging Area Configuration message to a Paging Agent,

specifying a list of paging area identifiers to be added or deleted.

When a Paging Agent receives a Paging Area Configuration message from a Tracking Agent, if the paging area identifiers specified in the received message is successfully added or deleted, it returns a Paging Area Configuration ACK message to the Tracking Agent.

4.12. LH-DMHA Authentication

All messages defined in this specification except for DMA Solicitation and DMA Advertisement messages MUST be authenticated. A DMHA-SA needs to be established between peers that exchange LH-DMHA messages covered with LH-DMHA authentication either directly or indirectly.

By default, HMAC-MD5 [HMAC-MD5] is used for calculating any type of authentication data.

Each LH-DMHA message has a message identifier which monotonically increases every time a message is transmitted from a node. A node that performs LH-DMHA authentication for a received message MUST check the message identifier of the message and MUST NOT accept the message if the message identifier is out of the expected range in order to protect the message from reply attacks.

The next two sections explains detail for LH-DMHA authentication.

4.12.1. Authenticating Paging Message

When a Paging message is originated from a Dormant Monitoring Agent, the Dormant Monitoring Agent MUST calculate two kinds of authentication data: End-to-end Authentication Data and Hop-by-hop Authentication Data. End-to-end Authentication Data is calculated by using the DMHA-SA established between the Dormant Monitoring Agent and Host. Hop-by-hop Authentication Data is calculated by using the DMHA-SA established between the Dormant Monitoring Agent and the Tracking Agent.

When a Tracking Agent or a Paging Agent receives a Paging message, it MUST calculate the Hop-by-hop Authentication Data by using the DMHA-SA established between the previous hop Agent and the receiving Agent. If the calculated Hop-by-hop Authentication Data is not exactly same as the received one, it MUST discard the message.

When a Tracking Agent forwards a Paging message, it MUST NOT modify the payload the message except for the Hop-by-hop Authentication Data. The Tracking Agent MUST recalculate Hop-by-hop Authentication

Data by using the DMHA-SA between Tracking Agent and Paging Agent.

When a Paging Agent forwards a Paging message, it MUST remove the Hop-by-hop Authentication Data before forwarding the Paging message. It MUST NOT modify the remaining part of the payload of the message.

When a Host receives a Paging message, it MUST calculate the End-to-end Authentication Data by using the DMHA-SA established between the

Dormant Monitoring Agent and Host. If the calculated End-to-end Authentication Data is not exactly same as the received one, it MUST silently discard the message.

4.12.2. Authenticating Other Messages

When a node sends a LH-DMHA message except for DMA Solicitation, DMA Advertisement and Paging messages, it MUST calculate End-to-end Authentication Data by using the DMHA-SA established between the originating node and destination node.

When the destination node receives this message, it MUST calculate End-to-end Authentication Data by using the DMHA-SA established between the originating node and destination node. If the calculated End-to-end Authentication Data is not exactly same as the received one, it MUST discard the message.

4.13. Supporting Multiple IP Addresses Per Hardware Address

In the case of IPv6, it is possible to assign multiple IP addresses for an interface of a Host. Or if the Host supports both IPv4 and IPv6 it is possible to assign one IPv4 address and one or more IPv6 addresses for the interface. In such cases, the Host MAY perform paging registration for different IP addresses with specifying the same hardware address. To support this, both Dormant Monitoring Agents and Hosts MUST be able to handle multiple IP addresses per hardware address.

More specifically, multiple IP addresses can be specified in a DMA Registration message, and a Dormant Monitoring Agent MUST be able to perform paging operation when it receives a paging trigger packet with regard to any of those IP addresses. And the Host MUST perform paging deregistration for all of those IP addresses when it wakes up for any of those IP addresses unless the hardware supports different dormant modes for different IP addresses associated with the same hardware address.

4.14. Supporting Multiple Hardware Addresses

A Host MAY be equipped with multiple radio interfaces (e.g., both Bluetooth and IEEE 802.11 interfaces). Each radio interface may be identified by a separate MAC address. The host MAY use a separate IP address for each of its radio interface. In this case, different radio interfaces on the same Host can be treated by the Dormant Monitoring Agent as different IP hosts, each identified by a separate IP address. That is, the Host can perform paging registration for

each radio interface separately with the Dormant Monitoring Agent. The Dormant Monitoring Agent can then maintain paging registration states for each interface in the same way it handles a single-interface Host.

On the other hand, a single IP address MAY be used for multiple or all of the radio interfaces of a multi-interface Host. In this case, the Dormant Monitoring Agent MUST be able to handle multiple hardware

addresses per IP address. The Host MAY register multiple hardware addresses for the same IP address. Since the interfaces on a Host may not all be connected to the network at any given time or location, the Dormant Monitoring Agent MUST send a copy of the Paging message to each hardware address registered for an IP address registered for an IP address. Upon receiving one or more Paging messages regardless from which interface or interfaces, at least one interface on the Host MUST wake up. The Host MAY choose to wake up all or any subset of its interfaces. How to determine which interface or interfaces should be waken up is an implementation issue and is out of the scope of this document.

4.15. Supporting Mobility Management Protocol

If a Host is a mobile node, it is able to move around while it is in a dormant mode, with changing L2 attachment points or L3 subnets but without changing its IP address.

It is possible for a Dormant Monitoring Agent to be co-located with a Home Agent of Mobile IP so that packets destined for the mobile Host's home address are captured at the Home Agent for triggering paging operation before it is forwarded to the care-of address, instead of having a Dormant Monitoring Agent at each last hop subnet in foreign networks. This is still consistent with the definition of Dormant Monitoring Agent because the mobile's home network is considered to be the last hop subnet in terms of home address. Alternatively, if inter-administrative domain paging is not allowed due to network management policies, a Dormant Monitoring Agent can be co-located with a Foreign Agent of Mobile IP.

Although the LH-DMHA protocol is independent of any mobility management protocol, each mobility management protocol SHOULD have a capability to reduce the frequency of mobility binding update while the Host is in dormant mode in order to enjoy the benefit of DMHA in terms of both power saving and reduced signaling message exchange. In addition, if a Host is running a mobility management protocol that has such a capability, the Host SHOULD perform an action which is specific to the mobility management protocol in order to reduce the frequency of mobility binding update (e.g., sending a Binding Update with a longer lifetime in the case of Mobile IPv6) before it enters a dormant mode, unless the network supports the capability of optimization for mobility management protocol described in section "Capability Set". If the network supports the capability of optimization for mobility management protocol, the lifetime of the mobility binding cache managed by the Mobility Agent co-located with Dormant Monitoring Agent can be automatically synchronized with the lifetime of paging registration. In this case, the Host is exempt

from performing an action which is specific to the mobility management protocol in order to reduce the frequency of mobility binding update. In this case, the Host MAY request the above optimization by including an Optimization Request TLV in a DMA Registration message (see section "Message Format").

4.16. Keep-Alive

In order to make sure that a peering Agent is up and running, an Agent MUST periodically send a Keep-Alive message and to each of its peering Agents, and the Agent that receives a Keep-Alive message from its peer MUST return a Keep-Alive ACK message to the peer if authentication is successful. This operation is referred to as keep-alive. Keep-alive operation MUST be performed between a Dormant Monitoring Agent and a Tracking Agent, and between a Tracking Agent and a Paging Agent. Keep-alive operation MUST be performed bi-directionally. In other words, if Agent A and B are peering Agents, both Agent A and B MUST periodically and independently send a Keep-Alive message.

If an Agent receives a correctly authenticated Keep-Alive ACK message from an expected peer with which a Session has not been established yet, a new Session is established for the peer.

If an Agent does not receive a correctly authenticated Keep-Alive ACK message for a specific period from its peer with which a Session has been established, it MUST tear down the Session and MUST erase all the states created as as result of message exchange with the peer.

If an Agent receives an LH-DMHA message except for a Keep-Alive message from a node with which a Session has not been established, it MUST be silently discarded without further processing.

4.17. Robustness Against Failure of Network Elements

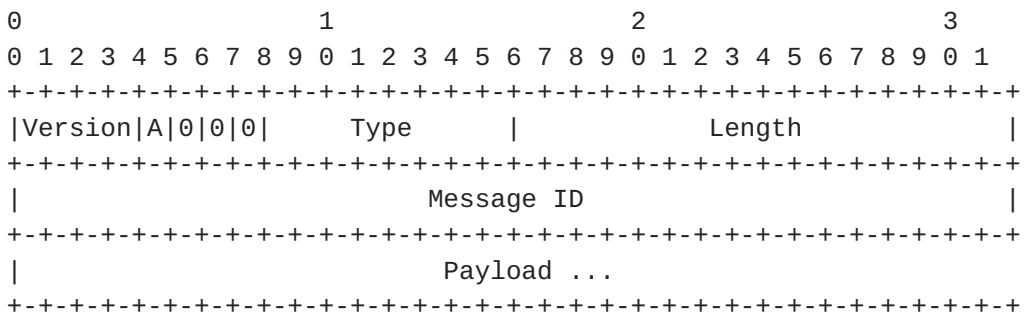
It is not desired at all for any protocol to have a single point of failure. LH-DMHA is not an exception. To increase robustness against failure of network elements, LH-DMHA allows for having multiple agents that perform the same task. For example, it is possible to have multiple Dormant Monitoring Agents within the same subnet. A Host can perform paging registration with any of those Dormant Monitoring Agents and switch to other Dormant Monitoring Agent anytime when it realizes that the currently registered Dormant Monitoring Agent is down.

It is also possible to have multiple Tracking Agents. Then, a Dormant Monitoring Agent can choose any of those Tracking Agent when sending a TA Registration message and switch to other Tracking Agent anytime when it realizes that the currently registered Tracking Agent is down.

It is also possible to have multiple Paging Agents serving the same paging area so that a dormant Host can receive Paging messages at least one of those Paging Agents.

5. Message Format

All messages defined in the LH-DMHA have the following structure.
All fields are transmitted in network byte order without padding.



The first 8 octets are the protocol header.

Version
The version of the protocol. The current version is zero.

A-flag

When this bit is set to be one, it indicates that an acknowledgment MUST be returned from the receiver of the message.

Type
Message type.

Length
Length of the Payload part in octets. The currently defined message types are shown in Table 1.

Message ID
This unsigned 32-bit field contains a monotonically increasing counter value (sequence number) given by the originator of the message. This is used for matching ACKs against requests as well as for replay protection. The Message ID is initialized to be zero when a node starts up or when the Message ID reaches its maximum value.

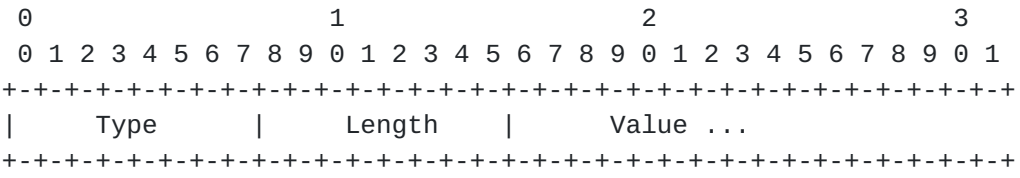
Table 1: Message Types

Type	Message Name	A-flag
0x01	DMA Solicitation	1
0x02	DMA Advertisement	0
0x03	DMA Registration	1
0x04	DMA Registration ACK	0
0x05	TA Registration	(see Note 1)
0x06	TA Registration ACK	0
0x07	Paging Area Advertisement	0
0x08	Paging	0
0x09	Paging Area Configuration	1
0x0a	Paging Area Configuration ACK	0
0x0b	Keep-Alive	1
0x0c	Keep-Alive ACK	0

Note 1: The A-flag for a TA Registration message MAY be set to 0 if the message is originated by a Host when the network supports the capability of "non-mandatory paging area update" described in section "Capability Set". Otherwise, the A-flag is set to 1.

5.1. Payload

The Payload part is composed of one or more TLVs (Type-Length-Value objects), where each TLV has the following format:



Type
The type of this TLV.

Length
The length of the Value field in octets.

Value
The value of this TLV. This field is null if the value of the Length field is zero.

A TLV can contain other TLV(s). In other words, TLV can be nested.

Each TLV can appear in any order in the Payload except for End-to-end Authentication Data TLV and Hop-by-hop Authentication Data TLV, which MUST be placed at the end of the message if included. If both an End-to-end Authentication Data TLV and a Hop-by-hop Authentication Data TLV are included in the message, the End-to-end Authentication

Data TLV MUST be placed before the Hop-by-hop Authentication Data TLV.

Table 2 summarizes the defined TLVs.

Table 2: TLVs

TLV Name	Type	Length
Address List	0x01	Variable
Dormant IP Address List	0x02	Variable
Dormant Hardware Address List	0x03	Variable
Lifetime	0x04	0x04
Lifetime Range	0x05	0x08
Status	0x06	0x04
Paging Trigger Packets	0x07	Variable
Capability Set	0x09	0x04
Request Message ID	0x0a	0x04
Paging Area List	0x0b	Variable
Terminal Identifier	0x0c	Variable
TA Address	0x0d	Variable
End-to-end Authentication Data	0x0e	Variable
Hop-by-hop Authentication Data	0x0f	Variable
Op-code	0x10	0x04
Optimization Request	0x11	0x00
Vendor Specific Extension	0x12	Variable
Extensible Paging Scheme	0x13	Variable

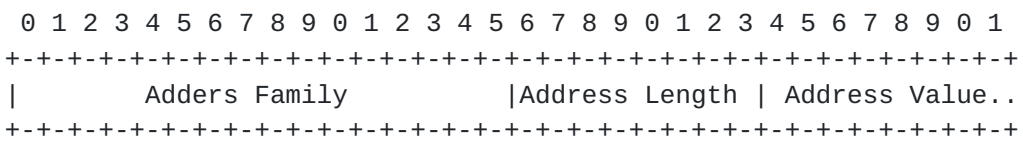
5.1.1. Address List TLV

This TLV contains either a list of IP addresses or a list of hardware addresses of the host that is performing paging registration. A sequence of Address fields are contained in the Value field of this TLV as follows:

Address 1
Address 2
.
.
.
Address N

Each Address field has the following structure.

0 1 2 3



Address Family

Two octet quantity containing a value from ADDRESS FAMILY NUMBERS in RFC1700 that encodes the address family of the address specified in this Address field.

Address Length
The length of the Address Value field in octets.

Address Value
The value of address.

5.1.2. Dormant IP Address List TLV

This TLV contains a list of IP addresses of the Host. The Value field contains an Address List TLV in which the list of IP addresses is specified.

5.1.3. Dormant Hardware Address List TLV

This TLV contains a list of hardware addresses of the Host. The Value field contains an Address List TLV in which the list of hardware addresses is specified.

5.1.4. Lifetime TLV

This TLV contains a lifetime of the paging registration, specified in seconds. The value of zero indicates paging deregistration.

5.1.5. Lifetime Range TLV

This TLV contains two lifetimes, the first one is the minimum lifetime and the second one is the maximum lifetime. Each lifetime contains 4-octet integer value specified in seconds.

5.1.6. Status TLV

This TLV contains a result of message processing. The Value field contains a one-bit flag (F-flag) for indicating a fatal error and a 31-bit integer for representing Status Code. If a message containing a Status TLV with a F-flag set to be one is sent to or received from a peering entity, the states created as a result of exchanging messages with the peer, including Session state, MUST be deleted immediately.

Detailed values for Status Code are defined in Table 3.

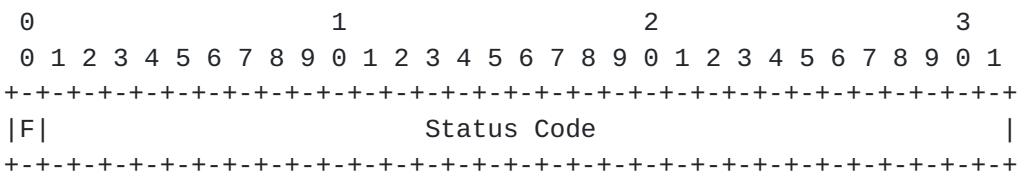

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|F|
Status Code

Table 3: Values for Status TLV

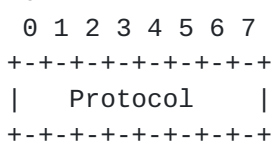
Status Name	F-flag	Status Code
Success	0	0x00000000
Unsupported Version	1	0x00000001
Invalid Header Flag	1	0x00000002
Unknown Message Type	0	0x00000003
Invalid Message Length	1	0x00000004
Unexpected Message ID	0	0x00000005
Unsupported TLV Type	0	0x00000006
Invalid TLV Length	1	0x00000007
Invalid TLV Value	0	0x00000008
Missing TLV	0	0x00000009
Resource Unavailable	0	0x0000000a
Unsupported Authentication Algorithm	1	0x0000000b
Unknown Terminal Identifier	0	0x0000000c
ICV Mismatch	0	0x0000000d
Session Lifetime Expired	1	0x0000000e
Unsupported Paging Scheme	0	0x0000000f

5.1.7. Paging Trigger Packets TLV

This TLV contains a set of paging trigger packets. The Value field of this TLV has the following format.

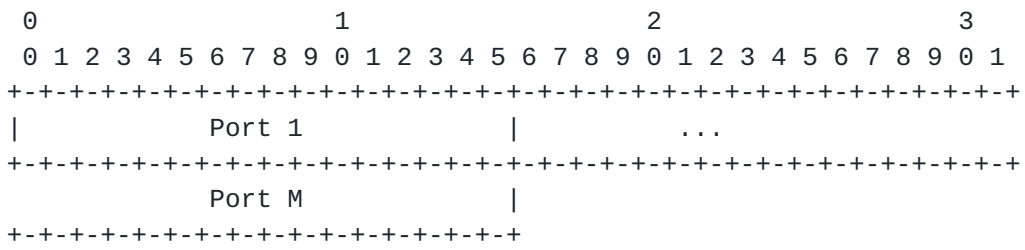
```
Protocol Number 1
Port/Type List 1
Protocol Number 2
Port/Type List 2
         .
         .
         .
Protocol Number N
Port/Type List N
```

Each Protocol Number field has the following structure.

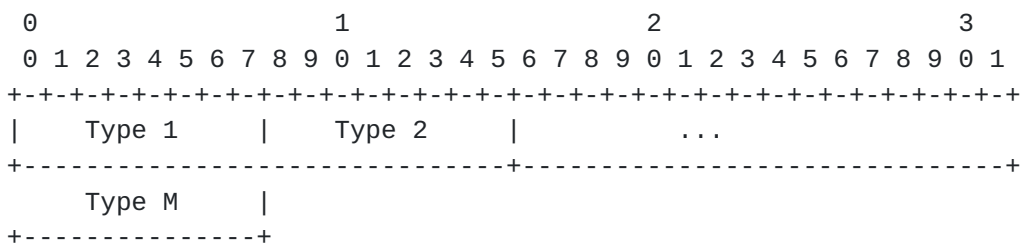


The Protocol field contains protocol number assigned by IANA, such as 0x01 (ICMP), 0x06 (TCP) and 0x11 (UDP).

If TCP or UDP is specified in the Protocol Number field, the Port/Type field contains a list of destination port numbers assigned by IANA, where the list of destination port numbers has the following format:

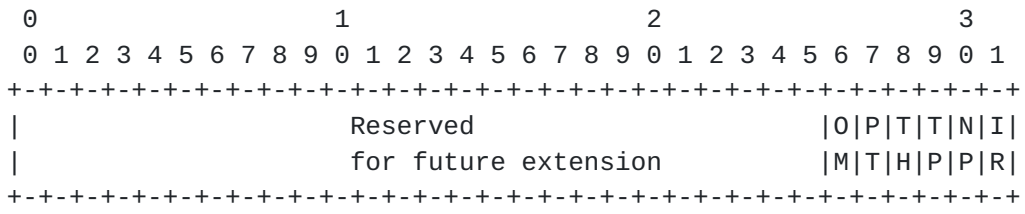


If ICMP is specified in the Protocol Number field, the Port/Type field contains a list of ICMP types assigned by IANA, where the list of ICMP types has the following format:



5.1.8. Capability Set TLV

This TLV contains a capability set of LH-DMHA. The Value field has 4-octet bitmap in which each bit corresponds to a specific capability as follows.



IR (Implicit paging registration)

If this bit is 1, a Host does not need to explicitly perform paging registration procedure before it enters a dormant mode. See section "Capability Set" for details.

NP (Non-mandatory paging area update support)

If this bit is 1, a Host can continue to be dormant when it crosses a paging area boundary.

TP (TA Registration from Paging Agent)

If this bit is 1, Paging Agents automatically perform paging area update operation on behalf of a Host when the Host performs L2 paging area registration.

TH (TA Registration from Host)

If this bit is 1, a Host is allowed to send a TA Registration message to a Tracking Agent to perform paging area update

operation.

PT (Paging trigger packets specified by Host)

If this bit is 1, a Host is allowed to specify a set of paging trigger packets in a DMA Registration message.

OM (Optimization for mobility management protocol)

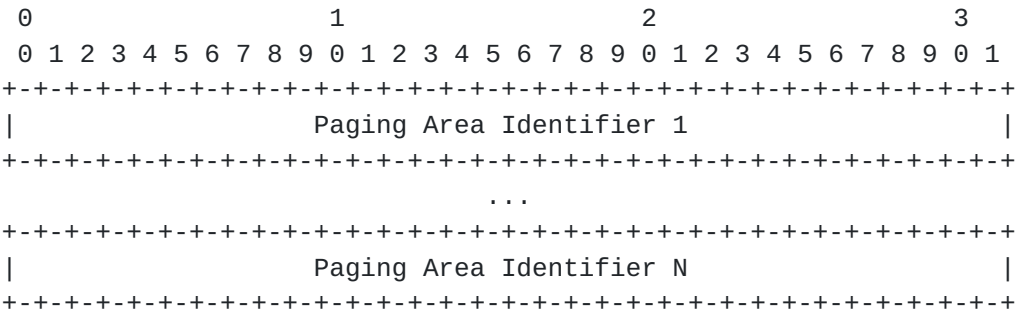
If this bit is 1, a Host is allowed to include an Optimization Request TLV in a DMA Registration message.

5.1.9. Request Message ID TLV

This TLV contains a 4-octet value of Message ID that was contained in DMA Registration or TA Registration messages. This TLV is contained in DMA Registration ACK or TA Registration messages and used by the receiver of the ACK to match the ACK against pending request.

5.1.10. Paging Area List TLV

This TLV contains a list of 4-octet identifiers which is used to identify paging area. The Value field of this TLV has the following format.



5.1.11. Terminal Identifier TLV

This TLV contains a terminal identifier that is used for identifying a DMHA-SA. The Value field of this TLV contains a single Address field for one of the IP addresses of the Host. See section "Address List" for the format of Address field.

If Host supports Mobile IP [MOBILEIP] or Mobile IPv6 [MOBILEIP-V6], the Home Address of the Host MAY be specified in this TLV.

5.1.12. TA Address TLV

This TLV contains an IP address of Tracking Agent. The Value field of this TLV contains a single Address field for one of the IP addresses of the Tracking Agent. See section "Address List" for the format of Address field.

5.1.13. End-to-end Authentication Data TLV

This TLV contains an Algorithm field which specifies the authentication algorithm and an Integrity Check Value (ICV) calculated against the message including the header and excluding this TLV and Hop-by-hop Authentication Data TLV if exists. If a Hop-by-hop Authentication Data TLV is also included in the message, the value of the Length field of the message header MUST be temporarily decreased by the number of octets of the Hop-by-hop Authentication Data TLV when calculating the ICV of the End-to-end Authentication Data TLV and the original value MUST be restored after calculating the ICV.

The Value field of this TLV has the following format.

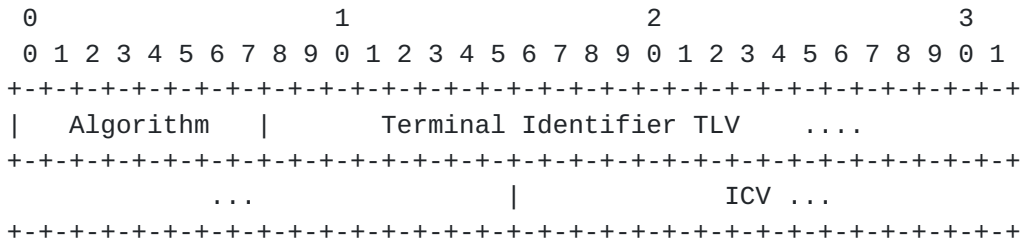


Table 4 describes the codes used in the Algorithm field.

Table 4: Algorithm Codes

Algorithm Name	Algorithm Code Value
HMAC-MD5	0x01

5.1.14. Hop-by-hop Authentication Data TLV

This TLV contains an Integrity Check Value (ICV) calculated against the message including the header and excluding this TLV. The Value field of this TLV has the same format as specified in End-to-end Authentication Data TLV.

5.1.15. Op-code TLV

This TLV contains a 4-octet integer operation code. The currently defined set of operation codes is shown in Table 5.

Table 5: Operation Codes

Operation Name	Operation Code Value
Add	0x01
Delete	0x02
Delete-all	0x03

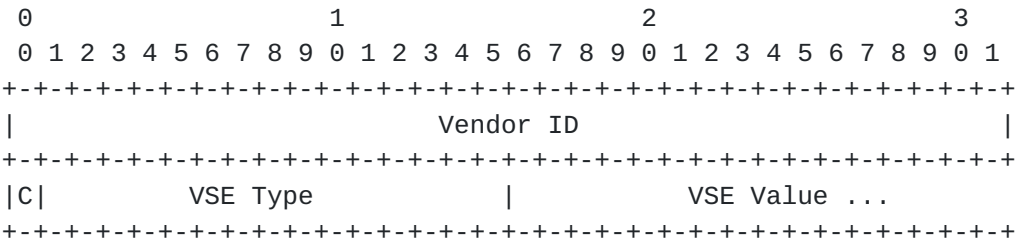
5.1.16. Optimization Request TLV

This TLV is used for requesting for the optimization for mobility management protocol, which is described in section "Supporting Mobility Management Protocol". This TLV MUST NOT contain a Value field and the value of the Length field MUST be zero.

5.1.17. Vendor Specific Extension TLV

This TLV contains information which is specific to a particular vendor's implementation.

The Value field of this TLV has the following format.



Vendor ID

The high-order octet is set to be zero and the low-order 3 octets contain the SMI Network Management Private Enterprise Code of the vendor in network byte order, as defined in RFC 1700.

C-flag (Critical flag)

If this bit is 1 and the receiving node does not recognize the contents of this TLV, the entire message MUST be silently discarded. If this bit is 0 and the receiving node does not recognize the contents of this TLV, only this TLV MUST be silently discarded and processing of remaining TLVs MUST be continued.

VSE Type

Indicates the particular type of this TLV. The administration of the VSE Types is done by the vendor.

VSE Value

Vendor specific data of this TLV. These data fields may be published in future RFCs. This field has zero or more octets.

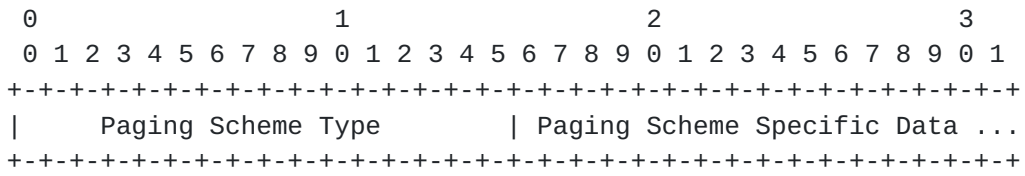
The length of this field can be computed from the Length field of this TLV.

5.1.18. Extensible Paging Scheme TLV

This TLV contains information which is specific to a particular location update and/or paging area configuration scheme but not

tightly coupled with a specific vendor. For example, information specified in [DPAC] MAY be carried in this TLV.

The Value field of this TLV has the following format.



Paging Scheme Type

This field contains an integer to distinguish a paging scheme type. Number assignment for this field must be done by IANA.

Paging Scheme Specific Data

This field contains information which is specific to the paging scheme type specified in the Paging Scheme Type field. The length of this field can be computed from the Length field of this TLV.

5.2. LH-DMHA Messages

5.2.1 DMA Solicitation Message

A DMA Solicitation Message contains no TLV.

5.2.2. DMA Advertisement Message

A DMA Advertisement message contains the following TLVs.

- Terminal Identifier TLV

  This TLV contains the terminal identifier for the Dormant Monitoring Agent that originates this message.

- Lifetime Range TLV

  This TLV contains the range of lifetime supported by the Dormant Monitoring Agent that originates this message.

- Capability Set TLV

This TLV contains the LH-DMHA capability set supported by the Dormant Monitoring Agent that originates this message.

o Vendor Specific Extension TLV [optional]

5.2.3. DMA Registration Message

A DMA Registration message contains the following TLVs.

- Dormant IP Address List TLV

  This TLV contains the list of IP addresses of the Host that is going to enter dormant mode.

- Dormant Hardware Address List TLV

  This TLV contains the list of hardware addresses that is associated with the IP address(es) specified in the Dormant IP Address List TLV.

- Lifetime TLV

  This TLV contains the requested lifetime of paging registration. When paging registration is performed, a lifetime of non-zero value MUST be specified. When paging deregistration is performed, a lifetime of zero MUST be specified.

- Paging Trigger Packets [optional]

  This TLV contains the set of requested paging trigger packets.

- Paging Area List TLV [optional]

  This TLV contains a list of paging area identifiers assigned to or chosen by the Host.

- Optimization Request TLV [optional]
  This TLV is included when the Host requests the optimization for mobility management protocol, which is described in section "Supporting Mobility Management Protocol".

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.4. DMA Registration ACK Message

A DMA Registration ACK message contains the following TLVs.

- Request Message ID TLV

This TLV contains the Message ID of the DMA Registration message to be acknowledged with this message.

- Dormant IP Address List TLV

  This TLV contains the list of IP addresses of the Host that is going to enter dormant mode.

- Dormant Hardware Address List TLV

  This TLV contains the list of hardware addresses that is associated with the IP address(es) specified in the Dormant IP Address List TLV.

- Lifetime TLV

  This TLV contains the accepted lifetime of paging registration.

- Paging Trigger Packets [optional]

  This TLV contains the set of accepted paging trigger packets.

- Paging Area List TLV [optional]

  This TLV contains a list of paging area identifiers assigned to or chosen by the Host.

- TA Address TLV [optional]

  This TLV contains the IP address of the Tracking Agent. The information is used when the Host performs paging area update operation by sending a TA Registration message directly to the Tracking Agent.

- Status TLV

  This TLV contains the result of paging registration operation.

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.5. TA Registration Message

A TA Registration message contains the following TLVs.

- Dormant IP Address List TLV

  This TLV contains the list of IP addresses of the Host that is going to enter dormant mode.

- Dormant Hardware Address List TLV

This TLV contains the list of hardware addresses that is associated with the IP address(es) specified in the Dormant IP Address List TLV.

o Lifetime TLV

This TLV contains the requested lifetime of paging registration. When paging registration is performed, a lifetime of non-zero value MUST be

specified. When paging deregistration is performed, a lifetime of zero MUST be specified.

- Vendor Specific Extension TLV [optional]
- Extensible Paging Scheme TLV [optional]
- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.6. TA Registration ACK Message

A TA Registration ACK message contains the following TLVs.

- Request Message ID TLV

  This TLV contains the Message ID of the TA Registration message to be acknowledged with this message.

- Dormant IP Address List TLV

  This TLV contains the list of IP addresses of the Host that is going to enter dormant mode.

- Dormant Hardware Address List TLV

  This TLV contains the list of hardware addresses that is associated with the IP address(es) specified in the Dormant IP Address List TLV.

- Lifetime TLV

  This TLV contains the accepted lifetime of paging registration.

- Paging Area List TLV

  This TLV contains a list of paging area identifiers assigned to the Host.

- TA Address TLV [optional]

  This TLV contains the IP address of the Tracking Agent, which is to be carried in a DMA Registration ACK message returned to the Host.

- Status TLV

  This TLV contains the result of paging registration operation.

- Vendor Specific Extension TLV [optional]
- Extensible Paging Scheme TLV [optional]
- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.7. Paging Area Advertisement Message

A Paging Area Advertisement message contains the following TLVs.

- Paging Area List TLV

  This TLV contains a list of paging area identifier advertised by the Paging Agent originating this message.

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

5.2.8. Paging Message

A Paging message contains the following TLVs.

- Dormant IP Address List TLV

  This TLV contains the list of IP addresses of the Host that is going to enter dormant mode.

- Dormant Hardware Address List TLV

  This TLV contains the list of hardware addresses that is associated with the IP address(es) specified in the Dormant IP Address List TLV.

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data calculated by the originating Dormant Monitoring Agent.

- Hop-by-hop Authentication Data TLV [optional]

  This TLV contains the authentication data calculated by the previous hop agent. If the previous hop agent is Paging Agent this TLV is not included.

5.2.9. Paging Area Configuration Message

A Paging Area Configuration message contains the following TLVs.

- Op-code TLV

  This TLV contains an operation code indicating "Add", "Delete", or "Delete-all". See section "Op-code" for the operation

code value for each operation code.

- Paging Area List TLV [optional]

  This TLV contains a list of paging area identifier to be added or deleted. This TLV MUST NOT be included when the operation code specified in the Op-code TLV indicates "Delete-all".

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.10. Paging Area Configuration ACK Message

A Paging Area Configuration ACK message contains the following TLVs.

- Request Message ID TLV

  This TLV contains the Message ID of the Paging Area Configuration message to be acknowledged with this message.

- Op-code TLV

  This TLV contains an operation code specified in the corresponding Paging Area Configuration message.

- Paging Area List TLV [optional]

  This TLV contains a list of paging area identifier that is successfully added or deleted by the Paging Agent that returns this message. This TLV MUST NOT be included when the operation code specified in the Op-code TLV indicates "Add-all" or "Delete-all".

- Status TLV

  This TLV contains the result of paging area configuration.

- Vendor Specific Extension TLV [optional]

- Extensible Paging Scheme TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.11. Keep-Alive Message

A Keep-Alive message contains the following TLV.

- Vendor Specific Extension TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

5.2.12. Keep-Alive ACK Message

A Keep-Alive ACK message contains the following TLV.

- Request Message ID TLV

  This TLV contains the Message ID of the Keep-Alive message to be acknowledged with this message.

- Vendor Specific Extension TLV [optional]

- End-to-end Authentication Data TLV

  This TLV contains the authentication data.

6. Protocol State Information

This section describes the state information maintained at each protocol entity.

6.1. Information Maintained by Host

6.1.1. Dormant Monitoring Agent State in Host

At least the following information is maintained per Dormant Monitoring Agent.

- The Terminal Identifier of DMA.
- The Terminal Identifier of Host.
- The shared secret for DMA.
- The content of Dormant IP Address List TLV.
- The content of Dormant Hardware Address List TLV.
- The content of Lifetime TLV.
- The contents of Request Message ID TLV contained in the most recently and correctly received DMA Registration ACK message.
- Message ID contained in the most recently sent DMA Registration message.

- The contents of TA Address TLV.
- The contents of Paging Trigger Packets TLV.
- The contents of Paging Area List TLV.

- The contents of Capability Set TLV.
- Retransmission timer for DMA Registration message.
- Timer for deleting this Dormant Monitoring Agent State entry.

6.1.2. Tracking Agent State in Host

At least the following information is maintained per Tracking Agent.

- The Terminal Identifier of TA which is also same as the the contents of TA Address TLV in the DMA State.
- The shared secret for TA.
- The contents of Request Message ID TLV contained in the most recently and correctly received TA Registration ACK message.
- The Message ID contained in the most recently sent TA Registration message.
- Retransmission timer for TA Registration message.

6.1.3. Paging Agent State in Host

At least the following information is shared among all Paging Agents.

- Shared secret for authenticating Paging Area Advertisement messages.

At least the following information is maintained per Paging Agent.

- The Terminal Identifier of PA.
- The Message ID contained in the most recently sent Paging Area Advertisement message.
- Timer for deleting this Paging Agent State entry.
- The content of Lifetime TLV.
- The contents of Request Message ID TLV contained in the most recently and correctly received DMA Registration ACK message.
- Message ID contained in the most recently sent DMA Registration message.

6.2. Information Maintained by Dormant Monitoring Agent

6.2.1. Host State in DMA

At least the following information is maintained per Host.

- The Terminal Identifier of Dormant Monitoring Agent.
- The Terminal Identifier of Host.
- The shared secret for Host.
- The contents of Dormant IP Address List TLV.
- The contents of Dormant Hardware Address List TLV.
- The contents of Lifetime TLV.
- The Message ID contained in the most recently and correctly received DMA Registration message.
- The Message ID contained in the most recently sent DMA Registration ACK message.
- The contents of TA Address TLV.
- The contents of Paging Trigger Packets TLV.
- The contents of Paging Area List TLV.
- The contents of Capability Set TLV.
- A flag indicating whether Optimization Request TLV is received from Host.
- Packet buffer for paging trigger packets.
- Retransmission timer for TA Registration message.
- Retransmission timer for Paging message.
- Timer for next round of paging operation
- Timer for deleting this Paging Agent State entry.

6.2.2. Tracking Agent State in DMA

At least the following information is maintained for a Tracking Agent.

- The Terminal Identifier of Dormant Monitoring Agent.
- The Terminal Identifier of TA.
- The Session state for TA.

- The shared secret for TA.

- The lifetime of this Tracking Agent State entry.

- The Message ID contained in the most recently and correctly received message from TA.

- The Message ID contained in the most recent message sent to TA.
- Retransmission timer for Keep-Alive message
- The timer for deleting this Tracking Agent State entry.

6.3. Information Maintained by Tracking Agent

6.3.1. Dormant Monitoring Agent State in TA

At least the following information is maintained per Dormant Monitoring Agent.

- The Terminal Identifier of DMA.
- The Terminal Identifier of TA.
- The Session state for TA.
- The shared secret for DMA.
- The lifetime of this Dormant Monitoring Agent State entry.
- The Message ID contained in the most recently and correctly received message from DMA.
- The Message ID contained in the most recently sent message to DMA.
- Retransmission timer for Keep-Alive message
- The timer for deleting this Dormant Monitoring Agent State entry.
- The list of Host States for dormant Hosts that is registered in DMA. Each Host State contains the following information on a particular Host.
  - The contents of Paging Area List TLV
  - The contents of Dormant IP Address List TLV.
  - The contents of Dormant Hardware Address List TLV.
  - The contents of Lifetime TLV.
  - The timer for deleting this Host State entry.

6.3.2. Paging Agent State in TA

At least the following information is maintained per Paging Agent.

- The Terminal Identifier of PA.
- The Terminal Identifier of TA.
- The shared secret for PA.

- The Session state for PA.
- The lifetime of this Paging Agent State entry.
- The Message ID contained in the most recently and correctly received message from PA.
- The Message ID contained in the most recent message sent to PA.

  /* Authors' note: If multicast is used for sending Paging messages, different Message ID spaces would be necessary for Paging messages and Keep-Alive messages. */

- Retransmission timer for Keep-Alive message
- The timer for deleting this Paging Agent State entry.
- The list of paging area identifiers to be advertised by PA.

6.4. Information Maintained by Paging Agent

6.4.1. Tracking Agent State in Paging Agent

At least the following information is maintained per Tracking Agent.

- The Terminal Identifier of TA.
- The Terminal Identifier of PA.
- The shared secret for TA.
- The Session state for TA.
- The lifetime of this Tracking Agent State entry.
- The Message ID contained in the most recently and correctly received message from TA.

  /* Authors' note: If multicast is used for sending Paging messages, different Message ID spaces would be necessary for Paging messages and Keep-Alive messages. */

- The Message ID contained in the most recent message sent to TA.
- Retransmission timer for Keep-Alive message
- The timer for deleting this Tracking Agent State entry.
- The list of paging area identifiers to be advertised by PA.

6.4.2. Host State in Paging Agent

At least the following information is shared among all Hosts.

o Shared secret used for creating Paging Area Advertisement messages.

6.4.3. Other States in Paging Agent

The following additional information MAY be maintained.

- o A list of Access Routers through which Paging messages are carried on traffic channel.

- o Any L2 dependent information needed for performing L2 paging. The L2 dependent information MAY include the list of Access Points that are not able to receive and process Paging messages at L3. Note that how to page Hosts through those Access Points depends on L2 and out of the scope of this document.

  /* Authors' note: if an Access Point is able to receive and process Paging messages at L3, then it can be a separated Paging Agent and SHOULD NOT be included in the above list. */

7. Security Consideration

LH-DMHA provides a method to authenticate message exchanges which is required for standard Seamoby IP Paging protocol [DMHA-REQ,DMHA-PROB]. For this purpose, LH-DMHA defines its own built-in authentication mechanism, called LH-DMHA authentication, which is used for authenticating LH-DMHA messages.

All the LH-DMHA messages exchanged directly or indirectly between the protocol entities except for DMA Solicitation and DMA Advertisement message MUST be authenticated by using the LH-DMHA authentication. The Security Association (SA) which is used for LH-DMHA authentication is referred to as a DMHA-SA.

Omitting authentication for DMA Solicitation and DMA Advertisement messages would not impact on the security aspect of LH-DMHA protocol, in that they do not contain important information except for Terminal Identifier of the Dormant Monitoring Agent contained in DMA Advertisement. Even if someone creates a DMA Advertisement message with a bogus Terminal Identifier, it does not matter because further message exchange (e.g., exchanging DMA Registration and DMA Registration ACK) between Host and Dormant Monitoring Agent is mutually authenticated. In addition, if paging registration operation fails several times due to receiving bogus DMA Advertisement messages, a Host is able to ignore subsequent DMA Advertisement messages advertised from the source. However, this protocol is vulnerable to attacks of sending DMA Advertisement messages with frequently changed bogus source IP addresses. Note that this kind of attack is common for all protocols such as DHCP, IPv6 Neighbor Discovery, etc., that may use unauthenticated multicast messages.

LH-DMHA does not provide a mechanism to establish the DMHA-SA. Instead, a number of methods could be used such as IKE, URP and statically shared key.

One of the main reasons for using LH-DMHA authentication instead of using IPsec is due to the difficulty for authenticating Paging messages at Hosts. There are two approaches to authenticate Paging

messages. One approach is based on hop-by-hop authentication in which Paging messages are authenticated at each hop by using the SA between the adjacent nodes of each hop (e.g., between DMA and TA, TA and PA, and PA and H). However, establishing such an SA between Paging Agents and a specific Host is difficult since the Host cannot determine the Paging Agent that will page it beforehand.

The other approach is based on authenticating Paging messages in different levels, one performed at each hop except for the one between Paging Agent and the Host, and the other performed in an end-to-end fashion by using the SA between Dormant Monitoring Agent and Host. The latter approach seems to be better because no SA is needed between Paging Agent and Host.

There are two choices in the latter approach regarding the layer in which end-to-end authentication is performed for Paging messages. The first choice is based on higher layer authentication mechanism (i.e., DMHA authentication). The second choice is based on IPsec with IP-in-IP encapsulation in which the inner IP packet containing a Paging message is covered by end-to-end IPsec AH (and the outer IP packet is used to route the packet along the "forwarding path" of the Paging message). Considering the fact that application level forwarding is needed for Paging messages, the first choice is better than the IP-in-IP based one, because in the case of IP-in-IP, forwarding is entirely performed at L3 and the contents of the inner packet are transparent at intermediate nodes (e.g., Tracking Agent and Paging Agent). Thus, IP-in-IP based approach is not suitable for carrying and authenticating Paging messages.

The other reason for using LH-DMHA authentication instead of using IPsec is that the IP address of the Host may change from that was used for paging registration when it performs paging deregistration or paging area update. If IPsec is used, a new IPsec SA needs to be established when the Host changes the IP address, which would increase signaling delay. If the Host uses Mobile IP or Mobile IPv6, and the Home Address of the Host is used for the identifier of the IPsec SA, a new IPsec SA would not have to be established when the Host changes its Care-of Address. However, in this case, the Host needs to perform mobility binding update in order for signaling packets to reach the Host, which would increase signaling traffic.

The DMHA-SA used for authenticating Paging Area Advertisement messages is a special SA for which the same shared secret MAY be shared among all Hosts and all Paging Agents. Such sharing is as a result of consideration of tradeoff between the security impact of bogus paging area advertisement and difficulty for establishing an SA between Paging Agents and a specific Host. Even a malicious user that is aware of the shared secret advertises bogus Paging Area Advertisement

messages, a dormant Host would not wake up as long as it also receives Paging Area Advertisement messages from correct Paging Agents, assuming that the Host waits for some time to correct a set of Paging Area Advertisement messages. Basically, a Host SHOULD NOT determine that it has crossed a paging area boundary immediately after receiving a Paging Area Advertisement message which includes a new paging area identifier, as multiple Paging Agents MAY advertise different paging area identifiers.

The only attack by using bogus Paging Area Advertisement messages is that it is possible to prevent a Host from exiting dormant mode even if the Host is actually out of the paging area. However, this attack would not be serious because it is possible only when the Host is mobile and both the Host and attacker is on the same shared media, which would be rare. If the attacker is not on the same shared media, there are three cases. First, for attackers from the edge subnets in the administrative domain, an access router is able to prohibit forwarding any Paging Area Advertisement message received on an interface to edge subnet(s). Second, for attackers outside the administrative domain, any Paging Area Advertisement message that is not originated from the administrative domain can be also filtered out. Third, for attackers inside the core network of the administrative domain, the attackers' network access can be physically prevented.

/* Authors' note : Based on the above discussion, authentication Paging Area Advertisement messages may not be necessary. */

8. References

[DMHA-PROB] J. Kempf, "Dormant Mode Host Alerting ("IP Paging") Problem Statement", RFC 3132, June 2001.

[DMHA-REQ] J. Kempf, et al., "Requirements and Functional Architecture for an IP Host Alerting Protocol", RFC 3154, August 2001.

[DPAC] P. Mutaf, et al., "DPAC: Dynamic Paging Area Configuration", Inter-Draft, Work in Progress, August 2001.

[HMAC-MD5] H. Krawczyk, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[IEEE802.11] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Std 802.11, June 1997.

[MOBILEIP] C. Perkins, "IP Mobility Support", RFC 2002, October 1996.

[MOBILEIP-V6] D. Johnson, et al., "Mobility Support in IPv6", Internet-Draft, Work in Progress.

[RAMJEE2001] R. Ramjee, et al., "IP Paging Service for Mobile Host", Proceedings of MOBICOM 2001, July 2001.

9. Authors' Information

Yoshihiro Ohba
Toshiba America Research, Inc.

P.O. Box 136
Convent Station, NJ
07961-0136
USA

Phone: +1 973 829 5174
Fax: +1 973 829 5601
Email: yohba@tari.toshiba.com

Nobuyasu Nakajima
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ
07961-0136
USA

Phone: +1 973 829 4752
Email: nnakajima@tari.toshiba.com

Tao Zhang
Telcordia Technologies, Inc.
445 South Street, Room 1J-214B
Morristown, NJ 07960
USA

Phone: +1 973 829 4539
Fax: +1 973 829 5889
Email: tao@research.telcordia.com

A. An LH-DMHA implementation over 802.11

A.1. 802.11 Power Management

The power management capability of IEEE 802.11 [IEEE802.11] for an infrastructure network can be summarized as follows. A station changing Power Management mode informs the Access Point (AP) of this fact using the Power Management bits in the Frame Control field of the transmitted MAC frames. An AP periodically broadcasts beacon signals to provide time synchronization information and inform stations in Power Save mode of arriving frames. A station uses the time synchronization information received from the AP to determine when it should wake up periodically from Power Save mode. The AP buffers the MAC frames destined to the station in Power Save mode and transmit them at designated times.

Unicast frames destined to a host in Power Save mode are transmitted by the AP and received by the station in different ways from broadcast/multicast frames. With every beacon transmission, the AP informs each station in Power Save mode of the unicast frames buffered by the AP for the station and whether these frames are to be sent to the station during a content-free or a contention time period. If a unicast frame is to be sent in a contention period, the station will poll the AP to receive the unicast frame. If a frame is to be sent during a contention-free period, the station will not poll the AP but will instead remain active until the frame is received or the contention-free period ends.

The AP notifies the stations of the existence of broadcast/multicast frames only via selected beacons periodically and the broadcast/multicast frames are sent immediately after these beacons.

A.2. Dormant mode support with 802.11 Power Management

By utilizing the timing differences for multicast/broadcast frames and unicast frames, three different dormant modes can be realized in the single Power Save mode.

- All Mode: Both unicast and multicast/broadcast frames are received.
- Unicast Only Mode: Only unicast frames are received.
- Multicast Only Mode: Only multicast/broadcast frames are received.

The dormancy levels of Unicast Only Mode and Multicast Only Mode are higher than that of All Mode. Unicast Only Mode is effective in terms of battery saving especially for a Host connecting to the network where broadcast/multicast traffic is high and most of the broadcast/multicast traffic is not important to the dormant station. On the other hand, there are also important broadcast/multicast frames that need to be received by the dormant Host in order to to receive

incoming SIP calls. One example is ARP REQUEST packets which are broadcast by a node in the last hop subnet in order to obtain the MAC address for an IP address of the Host.

Section A.3 describes an implementation of the Last Hop IP Paging Protocol that allows a Host to stay in the Unicast Only Mode while in power saving mode and will still be able to receive both unicast and selected types of broadcast traffic.

A.3. LH-DMHA over 802.11: Host Implementation

The LH-DMHA over 802.11 for IPv4 is implemented in a Host in the following way.

1) The Host monitors its own IP activity.

2) The Host stays in active mode while IP packets are sent or received.

3) If no IP packet is sent or received during a certain period, it performs paging registration.

4) If paging registration is successful, the Host enters the Unicast Only Mode, otherwise, enters the All Mode.

5) If the Host receives a paging trigger packet as a result paging, it performs paging deregistration.

A.4. LH-DMHA over 802.11: Network Implementation

In this section, it is assumed that a Dormant Monitoring Agent is co-located with Tracking Agent and Paging Agent in a single node and is referred to as a Paging Server. The Paging Server is assumed to be connected to the last hop subnet through wired Ethernet.

The LH-DMHA over 802.11 is implemented in a Paging Server in the following way.

1) The Paging Server monitors packets on the last hop subnet.

2) If it captures a paging trigger packet for a registered Host, it forwards the packet to the Host to registered hardware address, with

specifying the hardware address of the registered Host as the destination MAC address and the Dormant Monitoring Agent's hardware address on the monitoring interface as the source MAC address.

For example, if the paging trigger packet is a broadcast ARP REQUEST message, the destination MAC address of the forwarded packet is changed from ff:ff:ff:ff:ff:ff to the hardware address of the

registered Host, and the source MAC address is changed from the original sender's hardware address to the Paging Server's hardware address on the monitoring interface. The body of the ARP REQUEST is not modified. Since the Host in operating in Unicast Only Mode, it can receive the unicast ARP REQUEST. Then, it returns an ARP REPLY to the original sender, not to the Dormant Monitoring Agent.

In addition, if the Paging Server is co-located with the last hop access router or gateway, there is also a case in which it receives a unicast IP packet that is destined for the dormant Host and needs to be forwarded from other interface to the last hop interface. In this case it can use the ARP cache entry as usual to forward the packet to the dormant Host, since the ARP cache entry is not deleted during the lifetime of the paging registration (see section 3.3).

B. RFC 3154 Conformance Check

B.1. Impact on Power Consumption

The LH-DMHA protocol minimizes impact on the Host's dormant mode operation, because it allows the Host to stay dormant without configuring IP address while it is roaming.
The LH-DMHA protocol conforms to RFC3154 with this regard.

B.2. Scalability

The LH-DMHA protocol is scalable to support millions of Hosts, because multiple Tracking Agents can exist in an administrative domain in a way that each Tracking Agent keeps track of an exclusive set of Hosts.
The LH-DMHA protocol conforms to RFC3154 with this regard.

B.3. Control of Broadcast/Multicast/Anycast

The LH-DMHA protocol provides a filter mechanism to allow a Host prior to entering dormant mode to filter which broadcast/multicast/anycast packets active a page by defining a default set of paging packets and allowing a Host to explicitly specify the set of paging trigger packets. This prevents the Host from awakening out of dormant mode for all broadcast/multicast/anycast traffic. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.4. Efficient Signaling for Inactive Mode

The LH-DMHA protocol supports inactive mode detection mechanism for

Hosts that are registered with Dormant Monitoring Agents. A back-off mechanism is defined to reduce the traffic volume of Paging messages for Hosts that are considered to be inactive. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.5. No Routers

The LH-DMHA protocol does not support alerting mobile routers.

The LH-DMHA protocol conforms to RFC3154 with this regard.

B.6. Multiple Dormant Modes

It is possible for a Host running LH-DMHA protocol to have multiple dormant modes. An example for such usage is described in Appendix "An LH-DMHA implementation over 802.11".
The LH-DMHA protocol conforms to RFC3154 with this regard.

B.7. Independence of Mobility Protocol

The LH-DMHA protocol is independent of any mobility protocol. It can also support stationary dormant Hosts.
The LH-DMHA protocol conforms to RFC3154 with this regard.

B.8. Support for Existing Mobility Protocols

The LH-DMHA works with any mobility protocol. The only requirement for existing mobility protocol is to have a capability to reduce the frequency of mobility binding update while the Host is in dormant mode in order to enjoy the benefit of DMHA in terms of both power saving and reduced signaling message exchange. In addition, the LH-DMHA protocol supports optimization for mobility management protocol in order to perform paging registration and mobility binding update at the same time in a single message. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.9. Dormant Mode Termination

Upon receipt of a page (either with or without an accompanying L3 packet), the LH-DMHA forces a Host to execute the steps in its mobility protocol to re-establish a routable L3 link with the Internet. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.10. Network Updates

The LH-DMHA has a paging area update mechanism in which Paging Agent advertises paging area information and a dormant Host is able to directly or indirectly inform Tracking Agent what paging area it is in when when it changes paging area. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.11. Efficient Utilization of L2

One of the design policies of the LH-DMHA protocol is utilizing underlying L2 paging mechanisms as much as possible. It is able for the LH-DMHA protocol to use L2 paging mechanism in paging operation and L2 paging area update mechanism in paging area update operation. In addition, the LH-DMHA has a mechanism to advertise a capability set in order to efficiently utilize L2. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.12. Orthogonality of Paging Area and Subnets

The LH-DMHA allows an arbitrary mapping between subnets and paging areas. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.13. Future L3 Paging Support

The LH-DMHA does not require L2 support for paging. For example, the LH-DMHA works over 802.11 LANs that do not have paging. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.14. Robustness Against Failure of Network Elements

The LH-DMHA protocol supports Keep-Alive mechanism between peering Agents. The protocol also supports for having multiple backup Agents in order to avoid creating a single point of failure. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.15. Reliability of Packet Delivery

The LH-DMHA runs over unreliable transport (i.e., UDP). However, it supports retransmission and acknowledgement mechanism at application layer in order to increase the level of reliable delivery of messages. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.16. Robustness Against Message Loss

The LH-DMHA protocol has retransmission and acknowledgement mechanism, it is fairly robust against message loss. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.17. Flexibility of Administration

The LH-DMHA supports automatic configuration of paging area identifiers to be advertised from Paging Agents. The configuration at each Paging Agent is controllable by Tracking Agents. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.18. Flexibility of Paging Area Design

LH-DMHA supports flexible design of Paging Areas. For example, it supports both fixed and dynamically customized Paging Areas. It provides ways for hosts and networks to exchange customized information regarding Paging Areas which in turn allows any current or future paging area composing algorithm to be for determining how

paging areas should be composed. DPAC is an existing paging area composing algorithm which is supportable in this protocol by using Extensible Paging Scheme TLV. It allows different paging area composing algorithms to be used in different parts of a network provider's network as well as in different network providers' networks. It supports arbitrary location update mechanisms and paging algorithms.

B.19. Availability of Security Support

LH-DMHA provides an authentication mechanism (LH-DMHA authentication) which is equivalent to the one provided by IPsec AH. LH-DMHA does not have a mechanism to encrypt messages, but allows the use of IPsec ESP if available. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.20. Authentication of Paging Location Registration

The LH-DMHA provides a way to authenticate LH-DMHA messages used for paging registration operation with replay protection. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.21. Authentication of Paging Area Information

The LH-DMHA protocol provides a mechanism for authenticating paging area information distributed by the Paging Agent. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.22. Authentication of Paging Messages

The LH-DMHA protocol provides a mechanism for authenticating Paging messages generated by Dormant Monitoring Agent and distributed by Paging Agents. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.23. Paging Volume

Since only authenticated Paging message is processed, neither access to any legitimate Host is denied nor performance of the Host is degraded. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.24. Parsimonious Security Messaging

The additional power consumption for authenticating the message at dormant Hosts depends on the calculation complexity of HMAC-MD5.

B.25. Noninterference with Host's Security Policy

The LH-DMHA does not impose any limitations on a Host's security policies.

B.26. Noninterference with End-to-end Security

The LH-DMHA protocol does not impose any limitations on a Host's ability to conduct end-to-end security. The LH-DMHA protocol conforms to RFC3154 with this regard.

B.27. Detection of Bogus Correspondent Nodes

The LH-DMHA protocol allows a Dormant Monitoring Agent for filtering out paging trigger packets originated from a specific set of correspondent nodes. The LH-DMHA protocol conforms to RFC3154 with this regard.

C. Main Changes from the Previous Version

- This appendix is added.

- Abstract is modified.

- In section "Terminology", the definition of "Last Hop Subnet" is modified.

- A new terminologies "Agent" and "Session" is added to section "Terminology".

- In section "DMA Discovery", a statement is added so that a Host is able to send a DMA Solicitation message whenever it wakes up from dormant mode for detecting a subnet change.

- In section "Advertising Paging Area Information", the first sentence is modified in order to indicate that paging area information advertisement is not mandatory.

- In section "Capability Set", the first sentence is changed from "A DMA Advertisement message contains a set of capabilities that is supported by the advertising Dormant Monitoring Agent" to "A DMA Advertisement message contains a set of capabilities that is supported by the network".

- In section "Capability Set", the word "Heuristic paging" is replaced with "non-mandatory paging area update" and more detailed description is added.

- In section "Capability Set", a new capability "optimization for mobility management protocol" is added.

- In section "Supporting Mobility Management Protocol", the usage of

the capability of optimization for mobility management protocol is added. According to this, a new TLV "Optimization Request" is added in section "Message Format".

o In section "Paging Area Update", a statement is added for the case

in which TA Registration ACK message is not necessary for a TA Registration message sent from a Host when the network supports the capability of "non-mandatory paging area update" described in section "Capability Set".

- In section "Message Format", A-flag is added in message header.

- In sections "DMA Registration Message", "DMA Registration ACK Message" and "TA Registration ACK Message" , a Paging Area List TLV is allowed to carry multiple paging area identifiers while only a single paging area identifier was allowed in the previous version.

- Sections "Keep-Alive", "Keep-Alive Message" and "Keep-Alive ACK Message" are added in order to support keep-alive.

- Sections "Configuring Paging Areas", "Op-code TLV", "Paging Area Configuration Message" and "Paging Area Configuration ACK Message", are added in order to support automatic paging area configuration.

- In section "End-to-end Authentication Data TLV", the format of End-to-end Authentication Data TLV is changed so that multiple authentication algorithms are supported in the future. However, HMAC-MD5 is the only algorithm supported by this protocol.

- In sections "End-to-end Authentication Data TLV" and "Hop-by-hop Authentication Data TLV", the calculation rule of ICV is changed.

- "Vendor Specific Extension TLV" is added.

- "Extensible Paging Scheme TLV" is added.

- Section "Protocol State Information" is added.

- More detailed explanation is added to Section "Security Consideration".

- Appendix "Support for Existing Mobility Protocols" are updated so that added capability of "optimization for mobility management

protocol" is reflected.

- Appendixes "Robustness Against Failure of Network Elements" and "Flexibility of Administration" are updated so that added capabilities of Keep-Alive and Paging Area Configuration are reflected.

- In appendix B, section for "Flexibility of Paging Area Design" was missing and thus added to the current version of document.