Internet Engineering Task Force
INTERNET DRAFT

Yunzhou Li
National University
of Singapore

5 November 1996

Proximity Proxies for Mobile Nodes and Mobility Agents (PPM)

draft-liyunzhou-mobileip-ppm-00.txt

Status of This Memo

This document is a submission to the Mobile-IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the mobile-ip@smallworks.com mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document aims to explore an approach for the interoperability testing of Mobile IP implementations across the Internet. It proposes client/server proximity proxies, two intermediate entities between the mobile node and the mobility agent. This model can be used to solve the problem addressed in the hierarchical foreign agents model. The document proposes to build a tunnel between proximity proxies using Tunnel Request and Tunnel Reply messages, and enable routing policies to the tunnel by using Proxy Update message and adding a bit in Agent Advertisement message.

Contents

1. Introduction

The mobile IP base protocol [1] allows mobile nodes to move from one point of physical attachment within the Internet to another. Under this physical attachment, it is difficult to test interoperability of a few Mobile-IP softwares over the Internet. For example, a mobile node running one Mobile-IP software is not able to connect to a foreign agent running another Mobile-IP software. Furthermore, a mobile node is not able to switch, over the Internet, from a subnet at one remote site to a subnet at another remote site.

The second problem to be addressed here is what the hierarchical foreign agents model [2] discloses and has solved. That is, each time the mobile node moves, a Registration Request message has to be approved by the mobile node's Home Agent. In cases where the home agent is far away, it may become too expensive or even impossible to complete these frequent registrations.

This document proposes Proximity Proxies for Mobile Nodes and Mobility Agents (PPM), as an extension to the base protocol, in anticipation to solve these two problems. Under the base protocol, a mobile node can change its physical attachment to various links while maintaining its Internet connection. The PPM model provides a tunnel attachment mechanism by introducing pairs of proximity proxies, intermediate entities between mobile nodes and mobility agents.

The proximity proxies are built on a client-server model. A client proxy has a physical attachment to and serves mobile nodes, and a server proxy has a physical attachment to and serves mobility agents. A mobile node is said to have a tunnel attachment to a mobility agent if, there is a tunnel between the client and the server, and the client and the server respectively act as proximity proxies to the agent and the mobile node. By proximity proxies, we mean they have proximity function not necessarily using Proxy ARP. Thus the server will be able to attract packets from the agent and tunnel them to the mobile node via the client. In the reverse direction, the client will be able to attract packets from the mobile node and tunnel them to the agent via the server.

Under this model, Mobile-IP tests over the Internet become feasible. Each mobile node can be constantly connected to a client. The client can frequently request to switch its tunnel from a server in a remote site to that in another remote site. Thus a mobile node can change its tunnel attachment from one remote agent to another. This model is also able to assist a mobile node in mobility diagnostic. Before a mobile node departs from its home subnet, it can have a client in control and diagnose whether the Internet connection to its destination will be broken or not.

Under this model, the second problem can be solved by properly deploying servers and clients. For example, a foreign agent and a server proxy can be deployed in an autonomous system (AS), but more clients can be deployed within the AS. The clients maintains constant tunnels with the server. A mobile node moves around in the AS but is always attached to the agent over a tunnel. Thus no mobile node necessarily re-registers a new binding or registers simultaneous bindings while moving within the AS. Later the document demonstrates that both the agent and the server are able to keep track of mobile nodes and thus act as exchangers in this "switching network".

Tunneling methods can be found in [4] and [5]. The document also allows to use other methods to build a tunnel, especially provided in a heterogeneous network. To synchronize bi-directional tunnel between client proxy and server proxy, a client is allowed to send a Tunnel Request message to the server, and the server responds with a Tunnel Reply message.

To get a client to be a proximity proxy to a mobility agent, the document requires the server to tunnel Agent Advertisement messages to the client. To get a server to be a proximity proxy to a mobile node, the mobile node is required to address Proxy Update messages to the server via a client. Proxy Update messages can be used by the mobility agent and the server to keep track of the mobile node.

To indicate an intent to receive Proxy Update or request more information, the document defines a P-bit in Agent Solicitation message and Agent Advertisement message, and allows to include Server Proxy extension and Client Proxy extension in Agent Advertisement messages and Proxy Update messages.

2. PPM Overview

2.1. Client/Server Proxy

The PPM model provides two new entities, client proxy and server proxy. These two entities are intermediate proximity proxies between mobile node and mobility agent.

A client proxy, in short, client, is an Internet node that is on a link, on which mobile nodes may visit. It is called "client" in that it may request a server to build a tunnel towards itself. The client may work as a proximity proxy to a mobility agent without necessarily using proxy ARP. The client should enable a routing policy so that packets for the agent can be routed to the tunnel.

A server proxy, in short, server, is an Internet node on a link, on which one or more mobility agents reside. It is called "server" in

that it can serve to build a tunnel towards a client upon its request.
The server may work as a proximity proxy to a mobile node without necessarily using proxy ARP. The server should enable a routing policy so that packets for the mobile node can be routed to the tunnel.

2.2. Client/Server Tunnel

A tunnel between a client and a server can be built using methods in [4] and [5], or other methods. Hereafter, it is assumed that a method in [4] or [5] is used, and thus the tunnel could be bi-directional.

The bi-directional tunnel should be built simultaneously. A client should build a uni-directional tunnel from the client to a server if and only if the server agrees to build a tunnel from the server to the client.

2.3. Tunnel Requst and Tunnel Reply Messages

Tunnel Request and Tunnel Reply messages are designed to synchronize building the bi-directional tunnel between a client and a server.

To build a tunnel, the client needs to know the IP address of the server. However, the discovery of server addresses is not the purpose of this document and should be specified elsewhere.

A client should maintain at least a tunnel to a server. Thus at the system startup, the client should send a Tunnel Request to a server. The client should retransmit Tunnel Request if it does not receive a Tunnel Reply in a reasonable time, until it reaches a maximum number of retransmissions. The client can build more tunnels to other servers if necessary.

Upon receipt of a Tunnel Request, the server should respond with a Tunnel Reply with a proper lifetime if the server can honor this request. The server should build a uni-directional tunnel to the client under the agreement with the client.

Upon receipt of a matched Tunnel Reply, the client should build a uni-directional tunnel to the server. Thus the building of the bi-directional tunnel is synchronized.

The bi-directional tunnel is valid within the lifetime granted by the server. The client should extend the lifetime by starting another transaction of Tunnel Request/Tunnel Reply before the tunnel expires.

2.4. Agent Solicitation Message

Agent Solictation messages are sent from mobile node to mobility agents via clients and servers. If a mobile node or a client turns on the P-bit in a solicitation, it means to know more information. A client or a server receiving such a solicitation should respectively append Client Proxy extension and Server Proxy extension to subsequent Agent Advertisement messages.

On receiving an Agent Solicitation message,

- a client should tunnel the message to all the associated servers; the client should set up a solicitation P-bit flag for the mobile node if the message comes with the P-bit set;

- a server should forward the message to a link on which mobility agents reside; the server should set up a solicitation P-bit flag for the client if the message comes with the P-bit set;

- an agent should respond with an Agent Advertisement message.

2.5. Agent Advertisement Message

Agent Advertisement messages are critical to clients. A client can enable a routing policy for an agent only if it receives an Agent Advertisement.

To encourage a mobile node to issue Proxy Update messages, the P-bit in advertisement should be turned on. If a mobility agent or a server turns on the P-bit, it means to know more information. A server or a client receiving such an advertisement should respectively append Server Proxy extension and Client Proxy extension to subsequent Proxy Update messages.

On receiving an Agent Advertisement,

- a server should tunnel the message to all the associated clients; if there is a solicitation P-bit flag for a client, the server should individually append a Server Proxy extension to the message for the client; the server should update the advertisement P-bit status for the agent with the P-bit in the message;

- a client should forward the message to the link on which mobile nodes may visit, and enable a routing policy so that, all packets addressed to the advertising agent can be tunneled to the server; the routing policy is valid within the advertisement lifetime in the message, and should be disabled upon its expiry;

  if there is a solicitation P-bit flag for a mobile node, the client should individually append a Client Proxy extension to the message for the mobile node; the client should update the advertisement P-bit status for the server with the P-bit in the message;

- a mobile node should update the advertisement P-bit status for the agent or the client with the P-bit in the message; the mobile node should send a Proxy Update message before starting a registration procedure if the advertisement P-bit status for the agent or the client is on.

2.6. Proxy Update Message

Proxy Update messages are critical to servers. A server can enable a routing policy for a mobile node only if it receives a Proxy Update message.

On receiving a Proxy Update message,

- a client should forward the message to the server, to which the client imposed a routing policy for the agent specifed in the message;

  the client should append a Client Proxy extension to the message if the advertisement P-bit status for the server is on;

- a server should enable a routing policy so that, all packets addressed to the mobile node (specified in the message) can be tunneled to the client, from which the message comes. The routing policy is valid within the lifetime specified in the message, and should be disabled upon its expiry.

  The server should append a Server Proxy extension to the message and forward the message to the agent (specified in the message) if the advertisement P-bit status for the agent is on;

- an agent may locate the relevant mobile node, and redirect mobile traffic to a relevant server if a change in the mobile node's attachment is detected.

3. PPM Message Formats

The PPM model defines three types of UDP messages, with the first one-octet defined as message type:

    32 = Tunnel Request Message
    33 = Tunnel Reply Message
    34 = Proxy Update Message

The PPM model also requires two minor changes: a new flag bit must be added to the Agent Solicitation message and the Agent Advertisement message, replacing a previously unused, reserved bit in the message.

3.1. Tunnel Request Message

Tunnel Request is used for a client to request a tunnel from a server to it. A client should maintain the tunnel or otherwise stop forwarding Agent Advertisements.

IP fields:

Source Address — Typically the interface address from which the message is sent.

Destination Address — Typically the IP address of the server.

UDP fields:

Source Port — <variable>

Destination Port — 434

The UDP header is followed by the fields shown below:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Reserved    |            Lifetime           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                          Identification                       +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

Type 32 (Tunnel Request)

Reserved sent as zero; ignored on reception.

Lifetime
The number of seconds remaining before the tunnel is considered expired. A value of zero indicates a request for disconnection. A value of 0xffff indicates infinity.

Identification
A 64-bit number, constructed by the client, used for matching Tunnel Requests with Tunnel Replies, and for protecting against replay attacks of tunnel messages.

Extensions
The fixed portion of the Registration Request is followed by one or more of the Extensions.

3.2. Tunnel Reply Message

A server returns a Tunnel Reply message to a client which has sent a Tunnel Request (Section 3.1) message. The Reply message contains the necessary codes to inform the client about the status of its Request, along with the lifetime granted by the server, which MAY be smaller than the original Request.

IP fields:

```
   Source Address        Typically copied from the destination
                         address of the Tunnel Request to which
                         the server is replying.

   Destination Address   Copied from the source address of the
                         Tunnel Request to which the server is
replying
```

UDP fields:

```
   Source Port           <variable>

   Destination Port      Copied from the source port of the
                         corresponding Tunnel Request
```

The UDP header is followed by the fields shown below:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Lifetime            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Identification                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

```
   Type     33 (Tunnel Reply)

   Code     A value indicating the result of the Tunnel Request.
            See below for a list of currently defined Code values.
```

Lifetime
If the Code field indicates that the server agrees to build the tunnel, the Lifetime field is set to the number of seconds remaining before the tunnel is considered expired. A value of zero indicates that the tunnel has been disconnected. A value of 0xffff indicates infinity. If the Code field indicates that the tunnel was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Identification
A 64-bit number used for matching Tunnel Requests with Tunnel Replies, and for protecting against replay attacks of tunnel messages. The value is based on the Identification field from the Tunnel Request message from the client.

Extensions
The fixed portion of the Registration Reply is followed by one or more of the Extensions.

The following values are defined for use within the Code field.

0 tunnel connected

64 reason unspecified
65 administratively prohibited
66 insufficient resources
67 client failed authentication
68 requested Lifetime too long
69 poorly formed message

Up-to-date values of the Code field are specified in the most recent "Assigned Numbers" [10].

3.3. Proxy Update Message

Proxy Update messages are used not only for server to enable routing policies, but for client, server and mobility agent to keep track of mobile nodes. A Proxy Update can be sent from a mobile node to a client, from the client to a server, and from the server to the agent in that order. A mobile node should issue Proxy Update periodically.

IP fields:

Source Address Typically the interface address from which the message is sent.

```
   Destination Address   Typically that of the client, the server or
                         the agent if the message is sent from the
                         mobile node, the client or the server,
                         respectively.
```

UDP fields:

```
   Source Port           <variable>

   Destination Port      434
```

The UDP header is followed by the fields shown below:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Reserved    |           Lifetime            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Home Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Agent Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

```
   Type     34 (Proxy Update)

   Reserved sent as zero; ignored on reception.

   Lifetime
            The number of seconds remaining before the mobile node is
            considered away from a client.

   Home Address
            The home address of the mobile node.

   Agent Address
            The mobility agent address at the interface towards the
            mobile node.

   Extensions
            The fixed portion of the Proxy Update is followed by one
            or more of the Extensions
```

3.4. Agent Solicitation Message

One bit is added to the flag bits in the Agent Solicitation message to indicate an intent to receive more information from subsequent Agent Advertisement messages.

Thus, the Agent Solicitation message under the PPM model is:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|P|                         Reserved                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Proxy (P)

The Proxy (P) bit is set by the mobile node or the client to indicate its intent to receive more information from subsequent Agent Advertisement messages.

3.5. Agent Advertisement Message

One bit is added to the flag bits in the Agent Advertisement message to indicate an intent to receive Proxy Update messages or to receive more information from subsequent Proxy Update messages.

Thus, the Agent Advertisement message under the PPM model begins as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Registration Lifetime      |R|B|H|F|M|G|V|T|P|  reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| (unchanged...)
+-+-+-
```

Proxy (P)

The Proxy (P) bit is set by the agent or the client to indicate its intent to receive Proxy Update messages, or by the server or the client to indicate its intent to receive more information from subsequent Proxy Update messages. A client MUST have this bit set when it forwards an Agent Advertisement message.

4. PPM Extension Formats

The PPM model defines the following Mobile IP message extensions:

112 = Server Proxy Extension
113 = Client Proxy Extension
114 = Mobile-Client Authentication Extension
115 = Client-Server Authentication Extension
116 = Server-Agent Authentication Extension

The PPM messages may include Mobile-Foreign Authentication extension defined in [1].

This section describes each of the new PPM message extensions.

4.1. Server Proxy Extension

The Server Proxy extension may be included in an Agent Advertisement message, or a Proxy Update message.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | No. of Agents | No. of Clients|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Server Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	112
Length	12
No. of Agents	The number of agents on the same link as the server.
No. of Clients	The number of clients associated with the server over tunnels.
Server Address	The IP address of the server proxy

4.2. Client Proxy Extension

The Client Proxy extension may be included in an Agent Advertisement message or a Proxy Update message.

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |     Length    | No. of Servers| No. of MNs    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        Client Address                         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type — 113

Length — 12

No. of Servers — The number of servers associated with the client over tunnels.

No. of MNs — The number of mobile nodes on the same link as the client.

Client Address — The IP address of the client proxy

4.3. Mobile-Cleint Authentication Extension

This extension MAY be present in Proxy Update messages from a mobile node to a client, in cases in which a mobility security association exists between the mobile node and the client.

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |     Length    |         SPI  ....
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        ... SPI (cont.)          |       Authenticator ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type — 114

Length — 4 plus the number of bytes in the Authenticator.

SPI — Security Parameter Index (4 bytes). An opaque identifier

Authenticator — (variable length)

4.4. Client-Server Authentication Extension

This extension MUST be present in Agent Solicitation messages, Agent Advertisement messages and Proxy Update messages between a client to a server. The document requires that a proxy security association must exist between the client and the server.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |         SPI  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ... SPI (cont.)          |       Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type   115

Length   4 plus the number of bytes in the Authenticator.

SPI   Security Parameter Index (4 bytes). An opaque identifier

Authenticator   (variable length)

4.5. Server-Agent Authentication Extension

This extension MAY be present in a Proxy Update message from a server to an agent, in cases in which a mobility security association exists between the server and the agent.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |         SPI  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ... SPI (cont.)          |       Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type   116

Length   4 plus the number of bytes in the Authenticator.

SPI   Security Parameter Index (4 bytes). An opaque identifier

Authenticator   (variable length)

5. Mobile Node Considerations

The PPM model requires that a mobile node keep looking at the P-bit and the source link address in received Agent Advertisement messages.

An advertisement without P-bit set is directly from a mobility agent. An advertisement with P-bit set is from either a mobility agent or a client.

A change in the source IP address of advertisement means that a different agent has been detected. But a change in the source link address means that a different client has been detected.

A mobile node is considered away from an agent if, the mobile node does not receive any advertisement from the agent IP address within the advertisement lifetime. A mobile node is considered away from a client if, the mobile node does not receive any advertisement from the client link address within the advertisement lifetime.

5.1. Sending Agent Solicitation

The mobile node MAY send an Agent Solicitation message with P-bit set to request more information from clients or agents.

5.2. Receiving Agent Advertisement

Once the mobile node receives an Agent Advertisement, it MUST update the advertisement P-bit status for the agent or the client with the P-bit in the message, and copy its source IP address and source link address.

If the P-bit status changes from on to off, the mobile node SHOULD stop sending Proxy Update messages. But if the P-bit status changes from off to on, the mobile node MUST send Proxy Update messages as in section 5.4.

If the agent table is empty before the mobile node receives this advertisement with P-bit set, the mobile node SHOULD send Proxy Update messages before attempting to register a binding.

5.3. Handover

When the mobile node considers itself away from the agent currently serving it, it SHOULD check its agent table to find another agent. If there is no more agent on the table, no further action SHOULD be taken. Otherwise, before the mobile node attempts to register a new binding with the new agent,

- if the client associated with the disappearing agent is still on the client table and also sends advertisements on behalf of the new agent, the mobile node SHOULD put the new agent address in the subsequent Proxy Update messages to this client;

- or otherwise, the mobile node MUST stop sending Proxy Update messages to this client, choose another client that is sending advertisements on behalf of the new agent, and send Proxy Update messages to the new client by updating with the new agent.

If the mobile node is not away from the agent currently serving it but away from the client currently serving it, it MUST stop sending Proxy Update messages to the client. It SHOULD search its client table for another client that is sending advertisements on behalf of the same agent. A failure in this search is an error and SHOULD be logged. If there is such a client, the mobile node SHOULD send Proxy Update messages to the new client by updating with the agent.

5.4. Sending Proxy Update

The mobile node SHOULD send Proxy Update messages

- before it attempts to register a binding and the P-bit status for the relevant agent or client is on; or

- if the mobile node is away from the client currently serving it, and has chosen a new client on the client table.

The lifetime in the Proxy Update is the time within which the mobile node is considered reachable to the client. The mobile node SHOULD send a new Proxy Update message before it is considered away from the client, unless the mobile node does not require the service from the agent via the client.

The mobile node MAY append a Mobile-Client Authetication extension to the Proxy Update messages if there exists the mobility security association between the mobile node and the client.

6. Client Proxy Considerations

A client works on behalf of mobility agents. It can be associated with an agent upon receipt of an Agent Advertisement message. To receive such an advertisement, a tunnel from a server to it SHOULD be built up by sending Tunnel Request message.

6.1. Sending Tunnel Request

At the system startup, A client SHOULD build up at least one tunnel to a server. The discovery of server addresses is not the purpose of this document, and SHOULD be discussed elsewhere.

To build a bidirectional tunnel between a client and a server, the client SHOULD send a Tunnel Request to the server. The client SHOULD include a desired lifetime in the Tunnel Request.

The client SHOULD retransmit Tunnel Request if it has not received a matched Tunnel Reply in a reasonable time. Failure in receipt of such a Tunnel Reply message after a maximum of retransmissions SHOULD be logged for further administrative option.

The identification SHOULD be implemented as a timestamp or a nonce specified in the base protocol [1].

The client SHOULD append a Client-Server Autentication extension to the Tunnel Request message. The PPM model requires that there be a proxy security association between the client and the server.

6.2. Receiving Tunnel Reply

Upon receipt of a Tunnel Reply, the client MUST check the validity of the message. The reply is valid if

- the UDP checksum is valid;

- the low-order 32 bits of the Identification field in the Tunnel Reply equals to the low-order 32 bits of the Identification field in the most recent Tunnel Request sent to the server; AND

- the reply include a Client-Server Autentication extension at the end and the Authenticator is valid.

An invalid reply SHOULD be discarded and an error SHOULD be logged.

If the code field indicates that the server refuses to build the tunnel because the lifetime is too long, the client MAY resend a Tunnel Request with a proper lifetime.

If the code field indicates that the server refuses to build the tunnel, but there already exists a tunnel to the server, the tunnel SHOULD remain until its expiry. The code SHOULD be logged.

If the code field is positive but the lifetime is zero, the client MUST remove the existing tunnel to the server if any.

If the server agrees to build the tunnel by granting a proper lifetime, the client MUST build or reset the unidirectional tunnel to the server. The tunnel is valid within the granted lifetime and SHOULD be removed upon its expiry. To extend the lifetime of the tunnel, the client SHOULD send a Tunnel Request message to the server a reasonable time before the tunnel expires.

6.3. Receiving Agent Solicitation

If the client receives an Agent Solicitation message, it SHOULD set up a solicitation P-bit flag for the mobile node if the message comes with the P-bit set, and MUST tunnel it to all the associated servers. The client MAY turn on the P-bit to request more information from servers.

The client SHOULD append a Client-Server Autentication extension to the solicitation message. The PPM model requires that there be a proxy security association between the client and the server.

6.4. Receiving Agent Advertisement

Upon receipt of an Agent Advertisement, the client MUST check the validity of the message. The advertisement is valid if

- the ICMP checksum is valid;

- it is received from a tunnel; AND

- the message includes a Client-Server Autentication extension at the end and the Authenticator is valid.

An invalid advertisement SHOULD be silently discarded.

If the client receives a valid Agent Advertisement message, it SHOULD update the advertisemnt P-bit status for the server with the P-bit in the advertisement. The client SHOULD forward the advertisement to the link on which the client serves mobile nodes. In the advertisement to be forwarded, the client MUST turn on the P-bit and strip off the Client-Server Authetication extension. If there is a solicitation P-bit flag for a mobile node, the client SHOULD individually append a Client Proxy Extension for the mobile node.

the client MUST additionally enable a routing policy so that all packets addressed to the advertising agent can be tunneled to the server from which the message comes. The routing policy is valid within the the advertisement lifetime and SHOULD be disabled upon its expiry.

6.5. Receiving Proxy Update

Upon receipt of a Proxy Update message from a mobile node, the client MUST check the validity of the message. The Proxy Update is valid if

- the UDP checksum is valid;

- there is a routing policy for tunneling to a server all the packets destined for the agent specified in the message; AND

- the Authenticator is valid if the message includes a Mobile-Client Autentication extension at the end.

An invalid Proxy Update SHOULD be silently discarded.

The client MUST forward a valid Proxy Update message to the relevant server. In the message to be forwarded, the client MUST strip off the Mobile-Client Authetication extension if any, and SHOULD append a Client Proxy extension if the advertisement P-bit status for the server is on.

The client SHOULD additionally append a Client-Server Autentication extension to the message. The PPM model requires that there be a proxy security association between the client and the server.

7. Server Proxy Considerations

A server works on behalf of mobile nodes. It can be associated with a mobile node upon receipt of a Proxy Update message. To receive such a message, a tunnel from a client to it SHOULD be built up by answering Tunnel Request with Tunnel Reply.

7.1. Receiving Tunnel Request

Upon receipt of a Tunnel Request, the client MUST check the validity of the message. The request is valid if

- the UDP checksum is valid; AND

- the message includes a Client-Server Autentication extension at the end and the Authenticator is valid.

An invalid request SHOULD be discarded and an error SHOULD be logged.

On receipt of a valid Tunnel Request message, the server SHOULD respond with a Tunnel Reply with lower 32-bit identification copied from the original request.

If the server is not able to honor the request, it SHOULD put a proper code in the reply.

If the server denies the request and remove the existing tunnel to the client, it SHOULD set the code to a positive value (0) and the lifetime to 0.

Otherwise, if the server agrees to build or reset a tunnel to the client, it SHOULD set the code to a positive value (0) and the lifetime to a value not greater than that in the original Request. The server MUST build a tunnel to the client if there is not such a tunnel, or reset the existing tunnel to the client with the granted lifetime. The tunnel is valid within the granted lifetime and SHOULD be removed upon its expiry.

7.2. Receiving Agent Solicitation

Upon receipt of an Agent Solicitation, the server MUST check the validity of the message. The solicitation is valid if

- the ICMP checksum is valid;

- it is received from a tunnel; AND

- the message includes a Client-Server Autentication extension at the end and the Authenticator is valid.

An invalid solicitation SHOULD be silently discarded.

If the server receives a valid Agent Solicitation message, it SHOULD set up a solicitation P-bit flag for the client if the message comes with the P-bit set, and MUST broadcast the message on the link connected to a mobility agent. The server MUST strip off the Client-Server Autentication extension from the broadcast message.

7.3. Receiving Agent Advertisement

Upon receipt of an Agent Advertisement message, the server SHOULD update the advertisement P-bit status with the P-bit in the message, and MUST tunnel the message to the relevant client if it is a unicast, or to all the associated clients if it is a broadcast. If there is a solicitation P-bit flag for a client, the server SHOULD individually append a Server Proxy extension for the client.

The server SHOULD append a Client-Server Autentication extension to the advertisement message. The PPM model requires that there be a proxy security association between the server and the server.

7.4. Receiving Proxy Update

Upon receipt of a Proxy Update message, the server MUST check the validity of the message. The Proxy Update is valid if

- the UDP checksum is valid;

- it is received from a tunnel; AND

- the message includes a Client-Server Autentication extension at the end and the Authenticator is valid.

An invalid Proxy Update SHOULD be silently discarded.

Upon receipt of a valid Proxy Update message, the server MUST enable a routing policy so that all packets addressed to the mobile node (specified in the message) can be tunneled to the client from which the message comes. The routing policy is valid within the lifetime specified in the Porxy Update message and SHOULD be disabled upon its expiry.

If the advertisement P-bit status for the agent is on, the server SHOULD forward the message to the agent. In this message, the server MUST strip off the Client-Server Autentication extension, SHOULD append a Server Proxy extension, and MAY append a Server-Agent Authetication extension.

8. Agent Considerations

In general, the PPM model does not impose more requirements to the mobility agent. But an enhancement to the agent is recommended.

8.1. Receiving Agent Solicitation

There is no further requirement and enhancement to this message for mobility agents.

8.2. Sending Agent Advertisement

A mobility agent MAY refuse to receive Proxy Update messages by turning off the P-bit in Agent Advertisement messages.

If the agent intends to keep track of mobile nodes, however, it SHOULD turn on the P-bit in Agent Advertisement messages.

8.3. Receiving Proxy Update

An mobility agent MAY silently discard a received Proxy Update message if it does not support the PPM model.

If the agent supports the PPM model, upon receipt of a Proxy Update message, the agent MUST check the validity of the message. The Proxy Update is valid if

- the UDP checksum is valid;

- the Authenticator is valid if the message includes a Server-Agent Autentication extension at the end.

An invalid Proxy Update SHOULD be silently discarded.

If the agent intends to keep track of mobile nodes, however, it SHOULD look into the message. Packets addressed to the mobile node SHOULD be sent to a server or the mobile node, from which a most recent Proxy Update was received. In addition, the agent SHOULD balance traffic load among servers by looking into Proxy Update messages.

9. Security Considerations

The security issue is open for further discussion.

References

[1] Charles Perkins, editor. IP mobility support. RFC 2002, October 1996.

[2] Charles Perkins. Mobile-IP Local Registration with Hierarchical Foreign Agents. Internet Draft, draft-perkins-mobileip-hierfa-00.txt, February 1996. Work in progress.

[3] W. Simpson. IP in IP Tunneling. RFC 1853, October 1995.

[4] Charles Perkins. IP Encapsulation within IP. RFC 2003, October 1996.

[5] Charles Perkins. Minimal Encapsulation within IP. RFC 2004. October 1996.

[6] David B. Johnson and Charles Perkins. Route Optimization in Mobile IP. Internet Draft, draft-ietf-mobileip-optim-04.txt, February 1996. Work in progress.

[7] David C. Plummer. An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addresses for Transmission on Ethernet Hardware. RFC 826, November 1982.

[8] J. B. Postel. User Datagram Protocol. RFC 768, August 1980.

[9] J. B. Postel, Editor. Internet Protocol. RFC 791, September 1981.

[10] Joyce K. Reynolds and Jon Postel. Assigned Numbers. RFC 1700, October 1994.

Author's Address

Questions about this memo can also be directed to:

Yunzhou Li
Department of Information Systems and Computer Science
National University of Singapore
Lower Kent Ridge Road
Singapore 119260

Work: +65 772-6891 (Y.C. Tay c/o)
Fax: +65 779-5452 (Y.C. Tay c/o)
E-mail: scip4166@nus.sg