Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on July 14, 2007.

Copyright Notice

Copyright (C) The Internet Society (2007).

Abstract

Mobile IPv4 is a standard mobility protocol that enables IPv4 device to roam between networks. The mobile device has the Mobile IP function to signal its location to the routing anchor, known as the Home Agent. However, there are many IPv4 devices without such capability due to various reasons. This document describes a solution based on Proxy Mobile IPv4, which enables some other entity
to provide mobility support on behalf of an unaltered and mobility-unaware IPv4 device.

Table of Contents

1. Introduction ................................................. 3
2. Conventions used in this document ........................... 3
3. Solution Benefits ............................................. 4
4. Overview of Proxy Mobile IPv4 ................................. 5
   4.1. Mobility Signaling for Mobile Station ................. 5
      4.1.1. Proxy Registration ................................. 6
      4.1.2. Resource Cleanup ................................. 8
   4.2. Establishment of Bi-Directional Tunnel .................. 9
5. Appearance of Being at Home Network .......................... 9
   5.1. ARP Considerations .................................... 9
   5.2. ICMP Considerations ................................... 10
   5.3. DHCP Considerations ................................... 10
   5.4. PPP IPCP Considerations ................................ 11
   5.5. Link-Local Multicast and Broadcast Considerations .... 11
6. Mobility Proxy Agent Operation ............................... 11
7. Home Agent Operation ......................................... 12
   7.1. Processing Registration Requests ....................... 12
8. Mobile Station Operation ..................................... 12
   8.1. Initial Network Access ................................ 12
   8.2. Moving to a New MPA ................................ 12
   8.3. Packet forwarding .................................... 13
   8.4. Moving to a Different Domain ......................... 13
9. IANA Considerations .......................................... 13
10. Security Considerations .................................... 14
11. Acknowledgements .......................................... 14
12. References .................................................. 14
Authors’ Addresses ............................................. 15
Intellectual Property and Copyright Statements .................. 16
1. Introduction

There are many IPv4 devices which don’t have or can’t be enabled with Mobile IP [5] functionality. For them, Proxy Mobile IPv4 provides mobility support without being “touched”. The scheme is based on an external node acting as a proxy Mobile Node that registers the location of the device and maintains reachability while the device is on the network. The Foreign Agent and Home Agent perform their normal roles. The following examples depict possible scenarios:

1. An Access Point or Base Station performs registration when a mobile station is associated on the airlink.
2. An Access Router or Foreign Agent performs registration when a mobile station is detected.
3. A wireless mobile termination device performs registration for an attached host.

In the first two cases, the proxy node is a network element and the signaling can be considered part of the mobility management function of the domain. The third case is when the proxy node moves along with the mobile device and may be considered as a part of the mobile device. Some could argue that this is not a proxy mode of operation because the Mobile Node is the wireless mobile termination device. But the Home Address is "owned" by the host, meaning that packets to and from this IP address is received and sent by this host, respectively. The wireless mobile termination device is providing mobility for this IP address unbeknownst to the host. An example of this is cdma2000’s Network Mode on the mobile termination unit. For cdma2000, the true Mobile IP mode would be the Relay Mode, which is when the host operates as the Mobile Node. Anyways, this mode of operation is well understood and commonly deployed. The aim of this document is to describe how the network elements can provide mobility management for the mobile devices.

2. Conventions used in this document

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

The following new terminology and abbreviations are introduced in this document and all other general mobility related terms as defined in Mobile IPv4 specification [5].
Mobility Station (MS)

Any IPv4 node that has the ability to physically access or roam across different networks. The Mobile Station does not have the Mobile IPv4 protocol stack.

Mobility Proxy Agent (MPA)

The Mobile IPv4 entity that offers proxy mobility service for a Mobile Station by performing registration function on the host’s behalf. As mentioned before, this may be the Access Point, Base Station, Mobile Terminal, Access Router, or Access Gateway.

3. Solution Benefits

Proxy Mobile IPv4 is designed to satisfy the requirements listed below. In addition, the solution leverages well-studied specification and highly available implementations. Only incremental enhancements are added to Mobile IPv4 protocol to enrich its breadth to support both client-based and network-based mobility. For example, a Home Agent can anchor Mobile Stations that have Mobile IP as well as the hosts without such capability.

The network-based Mobility Management solution defined in this document provides the following benefits:

1. Support for Unmodified Hosts

An overwhelming majority of IPv4 hosts do not have Mobile IP capability. Providing mobility for them is achievable using Proxy Mobile IPv4. This is accomplished without "touching" the user’s devices running on a myriad of operating systems and networking stacks.

2. Airlink Consumption

Mobility-related signaling over the air-link is eliminated. Considering that Network Address Translation (NAT) is ubiquitous in IPv4 networks, a mobile node needs to send keepalives at short intervals to properly maintain the NAT states [6]. This can be performed by the MPA in the network which doesn’t consume any air-link bandwidth.
3. Reduction of Signaling Overhead in the Network

The MPA can aggregate multiple MSes on the same tunnel. Thus the frequent keepalives needed to maintain the NAT states can be reduced significantly. The signaling load on the network diminishes which increases the overall capacity.

4. Support for Heterogeneous Wireless Link Technologies

One aspect is how to adopt the scheme to an access technology. Since Proxy Mobile IPv4 is based on a heterogeneous mobility protocol, it can be used for any type of access network.

The other aspect is how to support roaming across different access technologies. As long as the MPA can use the same NAI to identify the MS for various access networks, roaming between them is possible.

5. Support for IPv4 and IPv6 Host

As IPv6 increases in popularity, the host will likely be dual stack. Adding IPv6 support to the host for Proxy Mobile IPv4 involves the methods defined in [10].

4. Overview of Proxy Mobile IPv4

4.1. Mobility Signaling for Mobile Station

After network access authentication, MPA exchange registration messages with the Home Agent to set up proper routing and tunneling of packets from/to the Mobile Station. As specified in RFC 3344 [5], a Foreign Agent may be used in the registration procedure. However, for the remainder of this document, MPA is described to use direct registration to the Home Agent. The difference is covered in RFC 3344 [5] and can be presumed to be adequately understood (e.g. the tunnel is between FA and HA instead of MPA and HA for FA registration and direct registration, respectively).
4.1.1. Proxy Registration

Description of the steps:

1a. MN performs L2 establishment with the base station (not shown) and performs access authentication/authorization with the AR. During this phase, the MN may run CHAP or PAP if PPP is used or EAP over foo (foo being the specific access technology or PANA). The AR acts as the NAS in this phase.

1b. The AR exchanges AAA messages with the AAA infrastructure to perform authentication and authorization of the MN. As part of this step, the AAA server may download some information about the MN (e.g. user’s profile, handset type, assigned home agent address, and other capabilities of the MN).

2. The MN sends an IPCP config request to the AR in case of PPP to request for an IPv4 address. If DHCP is used, the DHCP client in the MN sends a DHCPDISCOVER message. It is assumed in this document that
the AR has a DHCP proxy/server function.

3. Triggered by step 2 the MPA in the AR sends an Mobile IPv4 registration request (RRQ) to the Home Agent. The Home Agent’s address if either received at step 1b from the Home AAA or it is discovered in an out of band way by the AR. The RRQ contains the Care-of Address (CoA) of the AR (collocated FA in this case). The HoA field is set to ALL-ZERO-ONES-ADDRESS. The RRQ may be protected by MN-HA authorization enabling extension. The derivation and distribution of the MN-HA or FA-HA key is outside the scope of this document.

4. The home agent registers the MN’s session and assigns an HoA. The home agent returns the HoA in the RRP.

5. The AR responds back to the MN with an IPCP config-NAK to suggest the IPv4 address which is the HoA from the HA. This happens in response to step 2. If DHCP was used at step 2, the AR/DHCP-proxy/server sends back a DHCPOFFER with the IPv4 address set to the received HoA.

6. At this step, regular IPCP/NCP procedures get completed and the MN’s IP stack is ready to receive or send IP packets. If DHCP is used, the regular DHCPREQUEST and DHCPACK messages are exchanged and the MN’s IP stack is configured with the assigned IPv4 address.
4.1.2. Resource Cleanup

<table>
<thead>
<tr>
<th></th>
<th>MS</th>
<th>New MPA</th>
<th>HA</th>
<th>Previous MPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Proxy Registration Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o-----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Update existing MBE for MS</td>
<td>Reg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o---------------------</td>
<td>Revocation</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Remove visitor entry for MS</td>
<td>Reg</td>
<td>Revoc Ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Proxy Registration Reply</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o&lt;-------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2: Registration Revocation for Previous MPA**

MPA which no longer serve the Mobile Station needs to remove any associated mobility states and relinquish resources which are no longer needed.

When the Home Agent receives a Proxy Registration Request for a Mobile Station with an existing MBE, a Registration Revocation [3543] is sent to the previous MPA (in steps #1 through #3). The previous MPA removes the visitor entry for the Mobile Station before sending acknowledgement to the Home Agent (in steps #4 and #5). In parallel, the Home Agent sends the Proxy Registration Reply to the new MPA (in step #6). At the end of sequence of events, only states for the MS are in the new MPA and the Home Agent.
4.2. Establishment of Bi-Directional Tunnel

After receiving a successful Registration Reply for the Proxy Registration Request, the MPA sets up a tunnel to the Mobile Station’s Home Agent.

The bi-directional tunnel between the MPA and the Home Agent allows packets to flow in both directions, while the mobile station is connected to its visited link. The tunnel endpoints are the LMAP and the Home Agent. All traffic to and from the Mobile Station is sent through this bi-directional tunnel.

While the MPA is serving a Mobile Station, it MUST be able to intercept all packets sent from the Mobile Station and forward them out the MPA-Home Agent tunnel created for supporting that Mobile Station. Typically, forwarding is based on Layer 2 information such as the source MAC address or ingress PPP interface. This allows MSes with overlapping IP addresses to be supported.

Any packets received on the tunnel from Home Agent, the MPA decapsulates before forwarding to the Mobile Station on its link. Typically, the forwarding is based on the Destination IP address and HA indicator such as tunnel interface identifier or HA address. This allows MSes with overlapping IP addresses to be supported.

5. Appearance of Being at Home Network

Since the Mobile Station is not aware of mobility and does not participate in handover signaling, the network elements deceive the host to believe that it is stationary yet directing its traffic to the location where it has actually moved. An unmodified host uses ARP [8] to learn the MAC address of other nodes on the subnet, obtains an IP address and other host configuration via DHCP [2], and sends link-local multicast/broadcasts. The network’s response to the host has to be equivalent to the situation when host is always on the home subnet.

5.1. ARP Considerations

For IEEE 802 type of access networks (e.g. WLAN, WiMAX), the Mobile Station sends ARP request for host and default gateway on its subnet. The purpose of maintaining an ARP entry is to allow the delivery of the packet from MS to the IP node on the link.

For Proxy Mobile IP, the objective is to get the packet from the MS to the Home Agent. For CNs with the same home network but roaming elsewhere, the HA will tunnel the packet to them. Otherwise, the HA
forwards the traffic via normal routing.

The method to deliver the packet to the HA depends on whether the MPA is on the BS or AR. If the MPA is in the Base Station, the ARP entry in the MS serves no purpose since the packet will be tunneled to the HA by the BS. If the MPA is in the Access Router, then the Base Station needs to rewrite the destination MAC address properly to reach the AR. Alternatively, a common MAC address - listened to by all participating AR - is sent to MS in response to an ARP Request.

MPA@BS:    MS <-> BS/MPA <==============> HA

MS has ARP entries for default gateway and hosts on subnet which are set to some pseudo MAC address that is never used.

MPA@AR:    MS <-> BS     <-> AR/MPA <===> HA

MS has ARP entries for default gateway and hosts on subnet which are set to some pseudo MAC address which is rewritten by BS or a common MAC address for ARs.

Figure 3: ARP Entry Management

5.2. ICMP Considerations

In some cases, the Mobile Station sends an ICMP Query [9] with IP TTL set to 1 destined to the default gateway. This check is used to detect if default gateway is still reachable on the link. The MPA should respond with ICMP Reply when it is providing mobility service.

5.3. DHCP Considerations

Proxy Mobile IP allows the Mobile Station to operate as a normal IPv4 host using the standard IP address configuration via DHCP.

the MS boots up and initiates DHCP. The rest of the procedure is as per the description under fig 1.
5.4. PPP IPCP Considerations

When MS access the network via PPP [3], LCP CHAP is used to authenticate the user. After authentication, the NAS (which is the LMAP) sends the proxy Registration Request to the Home Agent, which responds with the Home Address in the Registration Reply. The NAS informs the MS to use the Home Address during IPCP [4]. When MS moves to a new NAS, the same procedure happens and MS has the same IP address for communication.

The message exchange is illustrated in fig 1.

5.5. Link-Local Multicast and Broadcast Considerations

MPA may tunnel all packets destined to Link-Local Multicast or Broadcast to the HA. The HA looks up the hosts which are in the same subnet and send a duplicated packet to each of them.

6. Mobility Proxy Agent Operation

The role of the MPA is performing the functions of a Mobile Node. It sends Registration Request to the Home Agent (via the Foreign Agent when available) to set up routing. When there is no FA, MPA operates in Collocated Care-of Address mode and provides tunneling support. FA can provide tunneling when it is used during registration in accordance to RFC 3344.

The MPA needs to know the following information for sending a registration.

1. NAI
2. MN-HA Mobility Security Association
3. Home Agent Address

This information can be downloaded from AAA server or configured by administrator. One example is configuration of subnet to HA mapping. When an MS associates with the Base Station, the MPA registers to the HA base on the IP address of the MS.
7. Home Agent Operation

The Home Agent has the functionalities described in RFC 3344. In addition, the following feature is introduced.

7.1. Processing Registration Requests

TBD.

8. Mobile Station Operation

As per this specification, a mobile station would function as a normal IPv4 host. The required behavior of the node will be consistent with the base IPv4 specification [1]. The mobile station will have the ability to retain its IPv4 address as it moves from one point of network attachment to the other without ever requiring it to participate in any mobility related signaling.

The mobile station when boots up for the first time can obtain an IPv4 address using DHCP.

As the mobile station roams, it is always able to communicate using the DHCP leased IP address on the home network. The MPA on the currently attached network signals to the HA to ensure proper forwarding path for MS’s traffic.

8.1. Initial Network Access

When the Mobile Station access the network for the first time and attaches to a network on the MPA, it will present its identity in the form of NAI to the network as part of the network access authentication process.

Once the address configuration is complete, the Mobile Station will always be able to use that IP address anywhere in network.

8.2. Moving to a New MPA

When a Mobile Station moves to a new MPA from another MPA, the following occurs:

The Mobile Station will perform a network access authentication with
the attached MPA. If the authentication fails, the Mobile Station will not be able to use the link. After a successful authentication, the MPA will have the identifier and the other profile data of the Mobile Station.

Once the network access authentication process is complete, the Mobile Station may sense a change in the Link Layer and use ARP, DHCP, and/or ICMP to detect if it is still on the same subnet. These mechanisms are handled by the network as described in section 5 "Appearance of Being At Home Network".

8.3. Packet forwarding

All packets that are be sent from the Mobile Station to the corresponding node will be sent as normal IPv4 packets setting the Source Address of the IPv4 header to the Home Address and the Destination Address to the corresponding node’s IP address. The default gateway for the Mobile Station will always be its HA. The ARP Entry for HA address is a pseudo HA MAC address.

Similarly, all packets sent to the Mobile Node’s Home Address by the corresponding node will be received by the Mobile Station in the original form (without any tunneling overhead) on its link.

No special operation is required by the Mobile Station to either send or receive packets.

8.4. Moving to a Different Domain

The scheme defined in this document, provides mobility support to the Mobile Station within that domain. Once the Mobile Station obtains an assigned Home Address, it can continue to use the same address roaming between MPAs in the network with its HA providing the topological anchor point for that address. However, the Mobile Station that roams across domains is required to have the Mobile IPv4 stack and operate as a normal MIPv4 mobile node to achieve mobility across domains.

9. IANA Considerations

TBD.
10. Security Considerations

The functionality in this document is protected by the Authentication Extensions described in RFC 3344 [5]. Each MPA needs to have the same MN-HA SA to register the MS. The SA can be provisioned by the administrator. The dynamic key distribution for this scheme is outside the scope of this document.

11. Acknowledgements

12. References


Authors’ Addresses

Kent Leung
Cisco Systems
170 West Tasman Drive
San Jose, CA  95134
US
Email: kleung@cisco.com

Gopal Dommety
Cisco Systems
170 West Tasman Drive
San Jose, CA  95134
US
Email: gdommety@cisco.com

Parviz Yegani
Cisco Systems
170 West Tasman Drive
San Jose, CA  95134
US
Email: pyegani@cisco.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA  01876
USA
Email: kchowdhury@starentnetworks.com
Full Copyright Statement

Copyright (C) The Internet Society (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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