Mobile IPv6 Working Group
Internet Draft
Expires: July, 2005

T. J. Kniveton
B. Patil
Nokia
S. Chakrabarti
Sun Microsystems
H. Petander
HUT
H. Soliman
Flarion
January, 2005

Mobile IPv6 Internet-based Remote Interoperability Testing Description
draft-kniveton-mipv6-remote-testing-01

Abstract

This document describes how implementors of Mobile IPv6 can use IPv6-based network facilities to perform remote testing of their

implementation with other groups participating in this testing program. The document aims to describe how one may become part of a testing group, what can be tested through this method, and the steps necessary to connect to remote Mobile IPv6 entities. This draft is

not meant for deployment, and no change in Mobile IPv6 implementation is needed in order to participate in testing.

Contents

1. Introduction

Throughout past years, various programmers have implemented Mobile IPv6 [?] based on the specification. Along the way, it became clear that some effort was necessary to ensure that different implementations could inter-operate and co-exist in a diverse and heterogeneous environment. In order to facilitate inter-operation, people in the Mobile IP community have organized events where implementors test their software against conformance tests, as well as testing with other implementors. Mobile IPv6 testing over the IPv6 Internet is an effort similar to 6-bone testing in the IPv6 development phase.

These events have been useful, and they continue to be important for running conformance tests and various interoperability tests that are not easily possible over MIPv6 Remote Interop Testing . Thus, this document does not seek to replace the regular interoperability events such as Connectathon [?] or ETSI [?]. The goal is that by using a distributed network testing model, it is possible to make faster progress on the Mobile IPv6 protocol [?] development, standardization and finally deployment.

This document describes the procedures on registering and configuring to test Mobile IPv6 base protocol over the IPv6 Internet. This document also assumes that implementors participating the remote testing event MUST support the Mobile IPv6 RFC 3775, and MAY support the companion IPsec spec, RFC 3776 (or their subsequent replacement RFCs).

2. Terms

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 [?].

In addition, this document uses terms as described by Mobile IPv6, such as Mobile Node, Home Agent, and Correspondent Node.

This terminology is intended to conform to those that have been used in IPv6, Mobile IPv6, Network Mobility, and other Internet protocols [?, ? , ? , ? , ?]

3. Requirements for test participation

3.1. Registration

All test participants including the Mobile IPv6 hosts sitting on the backbone need to register for testing (see section 5).

3.2. Implementation conformance; draft/RFC version

Many implementations of Mobile IPv6 exist, each with their own set of supported features, and according to a specific draft version of the specification.

For the purposes of this test network, it is assumed that the nodes in use will comply with the latest version of the specification, draft 24, or later.

3.3. Technical contact

It is necessary to supply a technical contact person who can be responsible for the registered Mobile IPv6 node. This is especially important for Home Agents, since they will presumably be continuously connected to the network to allow Mobile Nodes to register with them.

The technical contact should be familiar with the implementation in use (or at least its configuration), and capable of debugging a non-functional setup, using packet filtering tools or whatever other means are optimal.

3.4. What can be expected of hosts offered for testing against

The service of providing registrations on the MIPv6 Test Network web site is intended to facilitate easy introductions for parties who would like to test their software with each other. However, for most people this will be an ancillary task, which can not take too much of their time.

As such, we hope that all participants will try to keep their nodes functional and possibly help in debugging, but there is no guarantee of cooperation from the participating individuals, if they are busy or unavailable.

4. IPv6 Networks / 6bone

The 6bone is an IPv6 testbed that started as a virtual network composed of IPv6 over IPv4 tunnels, and is gradually transitioning to native IPv6 links. For those lucky enough to have a native IPv6 connection, all that will be needed is some way to obtain a global IPv6 address, either through address autoconfiguration [?], or some other means.

The 6bone is being gradually phased out as native IPv6 is added to the Internet [?]. If the user is in an environment where native IPv6 connections are available, this section can be skipped. For hosts that are not directly connected to the IPv6 Internet, a 6-over-4 tunnel with a tunnel broker will be necessary; to establish this, there are a couple of possible means. First, Freenet6 [?] will offer users their own /64 or /48 prefix, and provides software which will create a virtual tunnel interface to the IPv6 connection. This tunnel endpoint can be established on the access router providing connectivity to the Mobile IPv6 node. If this does not work, a tunnel can be manually established with a tunnel broker.

Other means of tunnel establishment include ISATAP [?] and Teredo [?], amongst others.

5. Registering for MIPv6 Test Network

The Mobile IPv6 remote testing is co-ordinated through a central administrator. Presently ETSI [?] has volunteered for the central

co-ordination. It is required that implementors interested in Mobile IPv6 register through the central co-ordinator to receive an account, address assignment for the test nodes. The key assignment for the mobile nodes can happen either through the central web-page or by contacting the Home Agent implementor contact person directly.

However, the central administration site should maintain a webpage which must include the steps to get an account, available Home Agents, Correspondent Nodes and Mobile Nodes and their addresses (see Section 5.3).

The webpage also lists contact information of a contact person of each implementation that volunteered to put a machine on the IPv6 Internet for remote testing. The central web page will be managed by ETSI [?].

5.1. Getting an Account

The central administrator wants to make sure that only valid Mobile IPv6 participants can access the central testing webpage and related information. Thus it is imperative to first get an account for the central web-site access. In order to receive an account, please follow the guidelines at http://mip6.plugtests.org. The web archives are available at http://list.etsi.org/plugtests-mip6.html

5.2. Registering Your MIPv6 Node(s)

Registering MIPv6 nodes happens according to the following guidelines:

5.2.1. Home Agent

Each participating home agent implementor is required to dedicate a home-agent node in the IPv6 Internet for interoperability testing purpose. Each home-agent implementation will list a contact person information in the web-page for key and address allocation to the mobile nodes. There may be some automated ways to receive the key from a home-agent node or implementor's site, but presently key and

address assignment are handled manually.

5.2.2. Mobile Node

There may be a few mobile nodes placed in the Internet for testing home agent functionality from a correspondent node. A mobile node should register through the central interoperability web page and get

it's home address from the home-agent implementor it wants to test with.

5.2.3. Correspondent Node

A correspondent node that offers route optimization in Mobile IPv6 can be a fixed node or a mobile node. A fixed correspondent node must register itself in the central webpage location with its IPv6 address in the Internet. It should also list a contact information for technical correspondence with the mobile node testers.

5.2.4. Mobile Router

[Currently this document does not address Mobile Routers]

5.3. Test web-page items

The Mobile IPv6 test network website will list the following items for the information exchange between the permanent Mobile IPv6 nodes and the implementation nodes that want to test against them. The items listed here are required information. However additional information may be listed as well.

5.3.1. Home Agent

- Company and contact information

- Home agent IPv6 address and the corresponding IPv4 addresses (if dual stack)

- List of home-addresses it assigns. This list must also indicate which home-addresses are presently used and which are available. Example:
  HOA1 (used by KEIO Univ.- contact name)
  HOA2 (available)

HOA3 (available)

- Security option supported
  - ESP or AH or None

- If IPsec is supported, specify encryption algorithm (ESP), authentication mechanism (AH), keys for each supported home-address(note this information may or may not be publicly listed), SPI information.

- List of other supported functionalities, for example: Return Routability message handling, Dynamic home agent discovery, Mobile Prefix Solicitation etc.

- Summary of logs: Each home agent that provides test service on the Mobile IPv6 test network must run as web-server as well. It is required to list a web URL of the log-file which provides current status of binding cashe of that home agent and possibly a packet flow staticstics on the corresponding HA-MN tunnels. The log-file may be updated in every half an hour approximately.

- Operating System and platform information

5.3.2. Correspondent Node

- Company and contact information

- IPv6 address of the node. If dual stack node, IPv4 address.

- If this node supports Return Routability protocol and any other route-optimization protocol.

- If this node supports mobile node or home agent functionality. If so, if that functionality is turned on.

- If this node supports IPsec protocol for regular traffic and wants to test interaction of IPsec-protected traffic with route-optimization, then it should list security association information depending on ESP or AH protocol support. (optional)

- A correspondent node that sits on the Mobile IPv6 test network, must run a web-service on it. It should list a URL of log-file. The log-file contains the binding cache information and possibly return routability message statistics for others to know which mobile nodes are being serviced through that node. The log-file should be updated in every half an hour.

- Operating system and platform information

5.3.3. Mobile Node

- Company and contact information

- Whether it can act as correspondent node as well

- If this node is placed on the Mobile IPv6 test network permanently, then it's IPv6 home address and care-of- address should be listed.

- Operating system and platform information

6. Security Associations

When a Mobile Node registers with a Home Agent, there must be a method for the MN to authenticate its identity to the HA. In MIPv6 Remote Interop Testing , there are three methods of authenticating the Binding Updates, listed here in increasing order of completeness.

The reason for allowing multiple levels of authentication is so that implementors can test their software in successive stages, before it is necessarily fully implemented. In operational environments, it is not recommended to ever allow unauthenticated BUs; however, in testing environments, it may be allowed in order to test other aspects of protocol operation.

6.1. Unprotected Binding Updates

In the simplest case, Binding Updates can be sent without any authentication. If an HA accepts unauthenticated HAs in the testing environment, it allows any MN to register from any Care-of Address, without proving its identity.

Although this is not desirable in a production setting, it is a valuable mode for testing purposes. As an implementation progresses, it may be useful to test mobility functionality before the security functionality is complete.

An HA in the testing network may choose whether it will accept unprotected BUs.

6.2. Authentication Header Protection

The Mobile IPv6 specification does not include information about Authentication Headers. However, many people have implemented Authentication Headers according to past specification. A companion specification may be submitted at a later time to specify how Home Agents should process these BUs.

Any Home Agent that already has an AH implementation may choose whether it wishes to continue accepting BUs protected by AH.

When the user that is testing a Mobile Node registers with the Mobile IPv6 Network Testing web site, it will be possible to request a static security association which will comprise a symmetric key using either HMAC-MD5, or HMAC-SHA1. This key will be provided by the web site along with a Home Address, and both should be added to the Mobile Node's configuration, so that it can be used in communications with the Home Agent.

6.3. IPsec ESP SA Protection

In the Mobile IPv6 IPsec companion draft [?], a method of using an IPsec ESP Security Association is described. This is the most secure method and is recommended over any other method. This would be the final stage of testing with respect to Binding Update security.

When IPsec SAs are used, the HA will pre-compute keys as in the previous Section, and the web site will contain this information along with the rest of the necessary information needed to describe an SA as shown in Section 5.2 of [?].

An HA may choose whether it wishes to accept BUs protected by IPsec ESP SAs (and it should choose ``yes'').

6.4. Pre-generating security keys for HA offered for testing

In order to facilitate automated key distribution by the web site, it will be necessary for Home Agent owners to pre-generate a certain number of keys and associate them with Home Addresses, so that when the web site delivers a (key,address) couple to the Mobile Node, the latter can immediately begin using it with either an Authentication Header or IPsec SA.

6.4.1. Adding to Web Site

To this end, the Home Agent owner should go through the steps necessary to generate these keys and Home Addresses, and provide them to the Mobile IPv6 Network Testing web site immediately after registering an Home Agent. The web site interface provides a means

for doing this.

7. Testing Configurations and Scenarios

There exist several possible test configurations. Each configuration requires that the initiator of the test knows the address of at least one other node. The first three subsections present test

configurations followed by mobility scenarios which can be used with configurations in which MN is being tested actively. The last subsection describes use of different kinds of network applications for testing of Mobile IPv6.

7.1. MN - HA

MN is tested actively with an online HA. Address of HA must be known, or if dynamic home agent address discovery is used the prefix of HA must be known to tester of MN. Details for the configuration of home address and SAs in MN are presented in sections 11.2 and 8. MN can also test communication with HA using any of the test applications.

Communications with public IPv6 enabled servers, such as www.kame.net, can be tested for testing of non-route optimized communications with CNs.

7.2. MN - HA - CN

MN is tested actively with an online CN. This configuration can have either a local HA or an online HA. Use of a local HA allows MN to move between its home network and a foreign network conveniently. If the HA is online, this scenario is an extension to the previous one.

The address of CN must be known to MN. Also the list of services running in CN must be known and the services accessible to the tester of MN.

7.3. CN - HA - MN

The CN can also be the actively tested entity. This requires that the home address of MN is known to the tester of CN and that MN is running some known service or services. MN should also be at a foreign network to make the test feasible or actively mobile during the test. Acticew mobility requires coordination of the testing.

7.4. MN1 - HA1 - HA2 - MN2

Testing of MN - MN communications is a special case of the MN - HA - CN test. Unless the testing is coordinated, one of the MNs, MN2, should be located at a foreign network and registered with a HA. The home address of MN2 needs to be known by tester of MN1, which would be the actively tested entity in this configuration. MN1 may use either the same HA as MN2 or a local HA, as in the MN - HA - CN case.

7.5. Mobility scenarios

Mobility can take different forms such as vertical handoffs, etc.. However, from the point of view of Mobile IPv6 interoperability mobility can be described by four scenarios and their combinations:

1. Foreign - foreign movement: MN starts in a foreign network and moves between foreign networks. This requires at least two foreign prefixes with the same scope as the home link, assigned to two links at location of MN testing.

2. Foreign - home movement: MN starts in a foreign network and moves to its home network. This requires MN and HA can be on the same link. The home link may be virtual, i.e., a tunnel, or physical, e.g., an ethernet segment. Also a foreign link with a prefix with the same address scope as home link is required.

3. Home - foreign movement: MN starts at home amd moves to a foreign network. This requires MN and HA can be on the same link. The link may be virtual, i.e., a tunnel, or physical, e.g., an ethernet segment. Also a foreign link with the same address scope as home link is required.

4. Simultaneous movement of MNs: Two MNs, which communicate with each other move at the same time. The movement of both MNs can be any of the three types described above. The simultaneous movement results in both MNs assuming that the other MN is at its old location, which may be an interesting test scenario. However, simultaneous movement requires coordination of the handoffs.

7.6. Test applications

Mobile IPv6 route optimization and tunneling can be tested with multiple types of applications. Connection oriented applications, such as HTTP, FTP and SCP can be used for testing session continuity over handoffs. UDP applications, e.g., echo can be used for testing connectionless communications and ICMP ping can be used for testing when there are no services available and also for testing of fragmentation with Mobile IPv6 by using echo packets larger than the

PMTU.

Use of applications, such as HTTP, FTP, SCP, SSH and echo requires configuration of the services on the node being connected to and at least with SSH and SCP, adding of users on the server node and communication of the usernames and passwords. The communication of this information is decribed in section XXX.

8. Virtual Home Link and MN returning home

NOTE: The techniques described here are used ONLY for testing purposes, to simulate returning home when a physical link connection is not possible. This is NOT intended for standardization or deployment, but is simply the description of an optional testing tool.

Since the Mobile Node must attach to the Home Link of the home network (where the Home Agent is located), there must be a way to simulate the Mobile Node on one tester's network returning home to the home link on another tester's network. In order to facilitate this, we describe a method of setting up a tunnel and virtual home link.

The home link at the Home Agent has to be a link separate from its upstream (towards the Internet) link. This can be either a physical link, or a virtual link (which can be trickier to configure in some environments).

In order to support the tunneling of data to the home link, the Home Agent and Mobile Node will need to establish a bi-directional tunnel between a new virtual link on the mobile node, and the virtual (or real) link at the Home Agent. Currently, there is no signaling mechanism to automatically configure this link, so it should be done using some tunnel brokering mechanism, or set through a static tunnel.

8.1. Tunnel Establishment

There is more than one way for the Mobile Node to switch from Visited Link (using Care-of Address and registering with HA) to Virtual Home Link (de-registering). However, there is one suggested method which will work with most operating systems and implementations, with only one physical interface connected to the IPv6 Internet, which is described in the following section.

8.2. Detecting the home link

The visited network will be represented by a physical interface, at least one of whose IPv6 addresses is the CoA. When the tester wants to trigger returning home, a tunnel will be created to the Home Agent. This will be connected to a virtual tunnel interface on the MN.

When the tunnel is established, the Mobile Node will detect Router Advertisements from the HA, and should then roam from the Visited

network (the upstream link it is using to get its Care-of Address) to the Virtual Home Network provided by the tunnel. The Home Agent (or Access Router connected to the same link) that provides the tunnel from the Home Network side must send Router Advertisements containing the prefix of the home network as normal.

The Home Agent should send both unsolicited RAs, and respond to router solicitations with solicited RAs, as described in Section 7.5 of [?].

When the Mobile Node sees these, it will know it has wandered (virtually) home, and de-register from the binding cache of the HA. In effect, it will ignore the visited network until the tunnel is no longer available and it has to roam to the (ever-present) visited link again.

9. Configuration

This section provides some information about how to configure the various Mobile IPv6 nodes in order to operate with this testing scheme.

9.1. Home Agent

The Home Agent should be placed behind an access router that has been delegated an IPv6 prefix refv6net and can provide address configuration services to the Home Agent.

The Home Agent needs to receive one globally-reachable IPv6 address to use as its Home Agent address, and a prefix of some size to use as the pool of addresses from which to assign Home Addresses. All of the aforementioned addresses should ideally be static and not subject to frequent change, for the sake of stability and so that these addresses do not need to be updated on the web site.

The Home Agent should assign its address to the network interface that has a direct connection to the access router (and subsequently the IPv6 Internet), and assign the prefix of Home Addresses to another link, which is the Home Link, that can either be a physical

network interface (if in the course of testing, the owner will be attaching Mobile Nodes to this Home Agent), or a virtual link.

Once the addresses are assigned, the owner should then proceed to generate (Home Address, security key) couples and register them on the web site6. It is optional to set up a tunnel broker so that the home network interface can be virtually connected to a Mobile Node for testing returning home and de-registration.

9.2. Mobile Node

The MN will first need to be manually configured with a home address derived from the remote home agent's prefix. In addition the MN needs to be configured with a security association with the home agent in order to secure binding updates. The security association can be established statically or dynamically. In the static case the MN will be provided with the following information:

- Authentication algorithm and key
- Encryption algorithm and key
- Security association lifetime
- The SPI
- The MN user will also need to configure the SPD.

It should be noted that the SPD is configured based on the information provided by the home agent operator. MNs must support IPsec ESP (transport mode) in order to protect binding updates sent to the home agent.

If a dynamic security association is feasible, the home agent must be configured with a certificate associated with the MN's home address. In this scenario both the MN and home agent need to support IKE.

Dynamic keying will enable the MN to test other Mobile IPv6 features like Mobile Prefix solicitation and advertisement messages that can be used to discover other home prefixes on the home link and allow the MN to test the SW operation when multiple home addresses are in use.

9.3. Correspondent Node

The correspondent node (CN) operation is described in section 9

of [?]. It is recommended that a CN for the purpose of testing Mobile IPv6 on the testbed implement the data structures and the capability to process mobility headers as described in section 9.

Any IPv6 node can be a correspondent node on the testbed. However it should be noted that the Mobile IPv6 specification has defined a new type of header called Mobility header which is used for route optimization signaling. Two types of CNs can be made available for testing:

1. A CN which implements the binding cache for mobility as well as the support for route optimization. This CN would be an IPv6 node that is compliant with the Mobile IPv6 specification [?].

2. A CN that does not implement the binding cache data structures or the route optimization feature. This is a mobility unaware IPv6 node. Such a node should still be capable of the packet processing requirements of all IPv6 nodes that are identified in section 9.3 of [?].

An MN can also play the role of a CN on the testbed. An MN can be a CN without necessarily having support for route optimization. However, it is strongly recommended that all IPv6 nodes should implement route optimization.

A correspondent node can be connected to the 6bone and obtain an IPv6 address as described in other sections of this I-D. For the test bed purposes it would be useful to have CNs that are of both types. These CNs would have static IPv6 addresses and advertised on the test bed web site. The CNs can offer HTTP service over IPv6 or enable FTP. If the CNs have the capability of logging the Mobile IP messages, it would be of benefit if these logs can be made available via http. This will make it easier to test Mobile IPv6 on the testbed.

10. Debugging and Web Service

It is recommended for debugging purposes that all CNs and HAs make their Mobile IPv6 log files avilable. To that end, the CNs and HAs that are registered on the Testing web site should run a web server which makes the system log and preferably an updated list of Bindings available. CN users can use this information to debug an unsuccessful registration attempt.

11. Firewalling and Security

Firewalls can be traversed to some extent, depending on the tunneling mechanism used [?, ?]. It is recommended that the Home Agent be directly accessible on the IPv6 Internet, and not behind a NAT or

Firewall.

11.1. Disclaimer About Security

It is the responsibility of any individuals or organizations participating in Internet-based Mobile IPv6 testing to ensure that their implementations and network configurations are sufficiently

secure and immune to attack. By the very nature of exposing nodes to the IPv6 Internet and to Mobile IPv6 signalling, an increased level of risk is present, and an opportunity for malicious attacks exists to some extent.

Myriad texts and informational materials exist which describe how to deal with and mitigate risks of the Internet. Information about Mobile IPv6-related risks are also well documented (e.g. see [?] Section 15).

If the potential participant(s) does not understand or feel comfortable accepting this risk, or if they are not capable of protecting their networks and nodes from malicious attacks, they should not participate in testing described in this document.

In no event will the authors of this document, operators of the MIPv6 Remote Interop Testing web site, IETF, or any other participants not involved in malicious attacks be liable for damage caused to any participant's nodes or networks. Caveat Emptor.

12. Appendix A

In Figure 1, HA1, HA2, CN_FX, CN_MN1 and CN_MN2 are Home Agents, fixed Correspondent Node (with route optimization) and Mobile nodes (with CN to MN route optimization functionality). These nodes are dedicated for the Mobile IPv6 test network and they should be available all the time to the test participants. Please see section 3 and section 5 for the requirements and registration of these nodes in the test network.

Test HA and Test MN(H) represent an HA test scenario over the Internet. It is recommended that test node HA should connect two interfaces to the IPv6 backbone and get two different prefixes. It should have a MN node for testing purpose. This MN node should be configured in one of the subnets and moved to other while it remains connected to CN_FX (for example). CN_FX is a dedicated correspondent node which provides route optimization functionality, but no mobile node functionality. Note that CN_FX machine may be configured to act as HA if the implementation offers the home agent functionality on the same box.

Similarly, a Test MN-CN first needs to get a home address (see section 5) from one of the dedicated HA machines and it then should plug into the IPv6 network. This will simulate movement and the test mobile node start registration process with that HA. Now the test CN-MN start a connection with CN-MN1(for example) and change its subnet in the IPv6 network. At this point, test CN-MN may start route-optimization with CN-MN1 in this example.

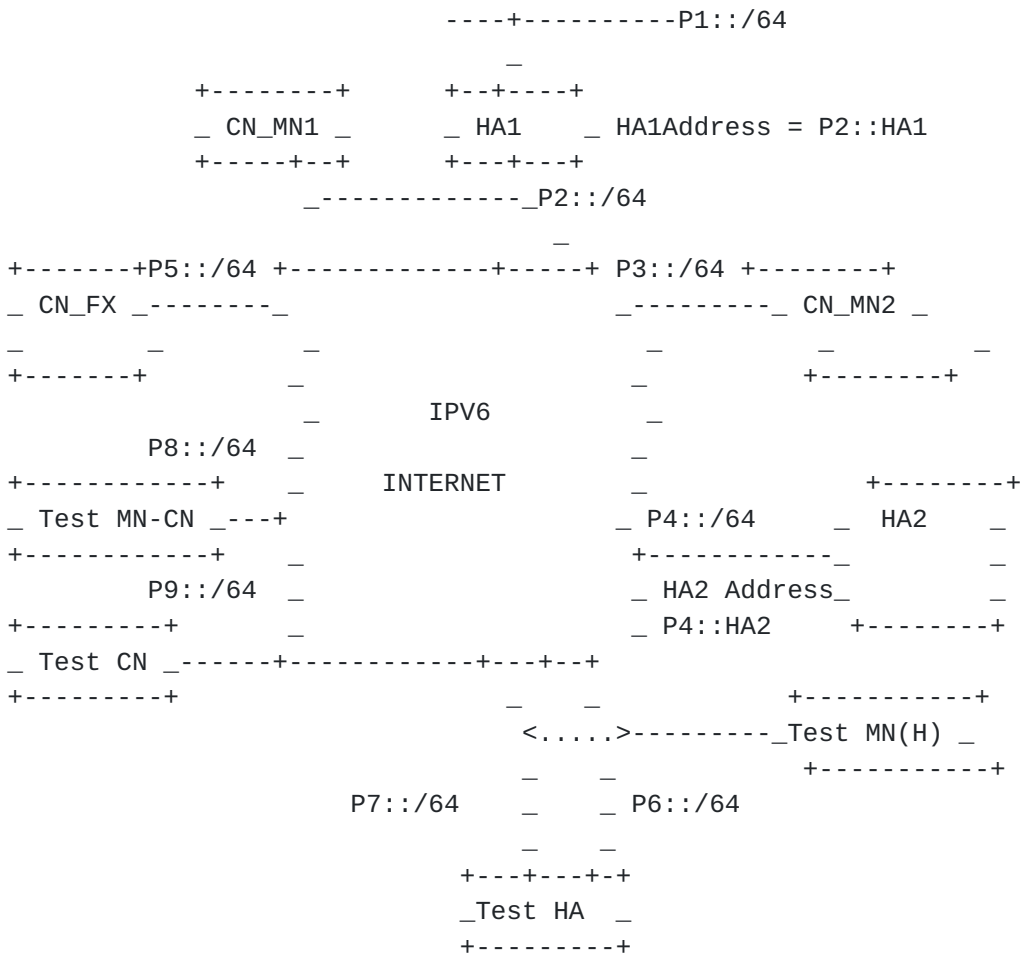

Figure 1: Example scenario of Base Mobile IPv6 Test Network

Thus for both mobile node and home agent testing,the test nodes should acquire two subnet prefixes from the IPv6 Internet. This test network can be used to study the advantage of route optimization as we can compare the round-trip-time for correspondent node in some subnet (with respect to the mobile node location, speed of link etc.) and the CN-MN located in the same subnet as with registered Home Agent.

A test CN node configuration is simple. It has to connect to the IPv6 Internet after acquiring a IPv6 prefix and then it should work with another Test-MN node to fire up route optimization functionality.

Please note that Figure 1 depicts an example scenario which can be used as a basic idea to develop the actual Mobile IPv6 test network. Please see section 7 for detailed discussion on test configurations.

13. IANA Considerations

The following protocol numbers may require allocation from IANA:

- None.

14. Intellectual Property Right Considerations

There are no known IPR issues with testing over the IPv6 backbone. Please see referenced documents for IPR considerations with respect to implementing those protocols.

"By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668."

15. Acknowledgements

The authors would like to thank ETSI organizers for agreeing to maintain the central co-ordination of the Mobile IPv6 Interoperability effort. Patrick Rene Guillemin has set up the preliminary central web page.

The authors would also like to thank the following individuals who have made suggestions to improve the text of this draft which were incorporated:

Vijay Devarapalli, Gabriel Montenegro, Hiroshi Miyata, and Connectathon 2003 MIPv6 participants for their interest and supporting ideas on Remote Mobile IPv6 testing. Finally, thanks to Erik Nordmark for originating the idea of remote Mobile IPv6 Testing through the Internet.

Authors' Addresses

T. J. Kniveton
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2025
E-mail: timothy.kniveton@nokia.com

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA
Phone: +1 972 894-6709
E-mail: basavaraj.patil@nokia.com

Samita Chakrabarti
Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, California 95054
USA
Phone: +1 650 786-5068
E-mail: samita.chakrabarti@sun.com

Henrik Petander
Helsinki University of Technology
Laboratory for Theoretical Computer Science
Konemiehentie 2, 02015 Espoo
Finland
Phone: +358 9 4515846
E-mail: henrik.petander@hut.fi

Hesham Soliman
Flarion Technologies
E-mail: h.soliman@flarion.com

Acknowledgement

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