MIP6
Internet-Draft
Expires: April 13, 2005

Alpesh. Patel, (Editor)
cisco Systems

October 13, 2004

# Problem Statement for bootstrapping Mobile IPv6
# draft-ietf-mip6-bootstrap-ps-01

## Status of this Memo



## Copyright Notice



## Abstract

A mobile node needs home address, home agent address and security association with home agent to register with the home agent. The process of obtaining this information is called bootstrapping. This document defines the problem for how the mobile can be bootstrapped in various deployment scenarios.

Table of Contents

1. Introduction . . . . . 3
1.1 Overview of the Problem . . . . . 3
1.2 What is Bootstrapping? . . . . . 4
1.3 Terminology . . . . . 4
2. Assumptions . . . . . 6
3. Design Goals . . . . . 7
4. Non-Goals . . . . . 8
5. Motivation for bootstrapping . . . . . 9
5.1 Addressing . . . . . 9
5.1.1 Dynamic Home Address Assignment . . . . . 9
5.1.2 Dynamic Home Agent Assignment . . . . . 10
5.1.3 Management requirements . . . . . 11
5.2 Security Infrastructure . . . . . 11
5.2.1 Integration with AAA Infrastructure . . . . . 11
5.2.2 Opportunistic or Local Discovery . . . . . 12
5.3 Topology Change . . . . . 12
5.3.1 Dormant Mode Mobile Nodes . . . . . 12
6. Network Access and Mobility services . . . . . 13
7. Deployment scenarios . . . . . 15
7.1 Mobility Service Subscription Scenario . . . . . 15
7.2 Integrated ASP network scenario . . . . . 15
7.3 Third party MSP scenario . . . . . 16
7.4 Infrastructure-less scenario . . . . . 17
8. Parameters for authentication . . . . . 18
9. Security Considerations . . . . . 20
10. Contributors . . . . . 22
11. Acknowledgments . . . . . 23
12. References . . . . . 24
12.1 Normative References . . . . . 24
12.2 Informative References . . . . . 24
Author's Address . . . . . 25
Intellectual Property and Copyright Statements . . . . . 26

## 1. Introduction

Mobile IPv6 [2] specifies mobility support based on the assumption that a mobile node has a trust relationship with an entity called the home agent. Once the home agent address has been learned either via manual configuration or via anycast discovery mechanisms, Mobile IPv6 signaling messages between the mobile node and the home agent are secured with IPsec. The requirements for this security architecture are created with [2] and the details of this procedure are described in [3].

In [2] there is an implicit requirement that the MN be provisioned with enough information that will permit it to register successfully with its home agent. The requirement to have this information statically provisioned creates practical deployment issues.

This document serves to define the problem of bootstrapping. Bootstrapping is defined as obtaining enough information at the mobile node, so that the mobile node can successfully register with an appropriate home agent.

The requirements for bootstrapping could consider various scenarios/ network deployment issues. It is the basic assumption of this document that certain minimal parameters (seed information) is available to the mobile node to aid in bootstrapping. The exact seed information available differs depending on the deployment scenario. This document defines/describes various deployment scenarios and provides for a set of minimal parameters that are available in each deployment scenario.

This document stops short of suggesting the various solutions to obtaining information on the mobile node. Such details will be available from separate documents.

### 1.1 Overview of the Problem

Mobile IPv6 [2] expects the mobile node to have a static home address, home agent address (or anycast address and do dynamic home agent discovery of Home Agent using ICMP messages) and a security association with a home agent (multiple home agents on the home network if dynamic home agent discovery is in use and multiple home agents are deployed.)

This static provisioning of information has various problems as discussed in Section 5.

The aim of this draft is to:

- Define bootstrapping.
- Identify sample deployment scenarios where MIPv6 will be deployed, taking into account the relationship between the subscriber and the service provider.
- Identify the minimal set of information required on the Mobile Node (and/or) in the network in order for the the mobile node to obtain address and security credentials, to register with the home agent.

## 1.2 What is Bootstrapping?

Bootstrapping is defined as obtaining enough information at the mobile node, so that the mobile node can successfully register with an appropriate home agent. Specifically, this means obtaining the home agent address, home address and security credentials for the mobile node and home agent to authenticate and mutually construct security credentials for Mobile IPv6 without requiring preconfiguration.

Typically, bootstrapping happens when a mobile node does not have all the information it needs to setup Mobile IPv6 service. This includes, but is not limited to MN not having any information when it boots up for the first time (out of the box), it does not retain any information during reboots, is instructed by the Home Agent (via some form of signalling) to do so etc.

Also, in certain scenarios, after the MN bootstraps for the first time (out of the box), subsequent bootstrapping is implementation dependent. For instance, MN may bootstrap everytime it boots, bootstrap everytime on prefix change, bootstrap periodically to anchor to an optimal (distance, load etc) HA, etc.

## 1.3 Terminology

For a complete introduction to terminology, please refer to [4].

General mobility terminology can be found in [4]. The following additional terms are used here:

ASP
: Access Service Provider. A network operator that provides direct IP packet forwarding to and from the end host.

IASP
: Integrated Access Service Provider. A service provider providing both network access and mobility. Referred to as IASP or ASP/MSP

in the document.

MSP
Mobility Service Provider. A service provider that provides Mobile IPv6 service. Granting such service requires authentication.

## 2. Assumptions

- A basic assumption in the Mobile IPv6 RFC [2] is that there is a trust relationship between the mobile node and MSP. This trust relationship can be direct, or indirect through, for instance, an ASP that has a contract with the MSP. This trust relationship can be used to bootstrap the MN.

  One typical way of verifying the trust relationship is using authentication, authorization, and accounting (AAA). In this document, two distinct types of AAA are considered:

  AAA for Network Access
  : This functionality provides authentication and authorization to access the network (obtain an address and send/receive packets).

  AAA for Mobility Service
  : This functionality provides authentication and authorization for mobility services.

  These functionalities may be implemented in a single entity or in different entities, depending on the service models described in Section 6 or deployment scenarios as described in Section 7.

- Yet another assumption is that some identifier, such as NAI, as defined in [7] or [8] is provisioned on the MN which permits the MN to identify itself to the ASP and MSP.

## 3. Design Goals

A solution to the bootstrapping problem has the following design goals:

- The following information must be available at the end of bootstrapping, to enable the MN to register with the HA.
  - MN's home address
  - MN's home agent address
  - IPsec SA between MN and HA or IKE pre-shared secret between MN and HA.
- The bootstrapping procedure can be triggered at any time.
- Subsequent protocol interaction (for example updating the IPsec SA) can be executed between the MN and the HA itself without involving the infrastructure that was used during bootstrapping.
- Solutions to the bootstrapping problem should not exclude storage of user-specific information on entities other than the home agent.
- Configuration information which is exchanged between the mobile node and the home agent must be secured using integrity and replay protection. Confidentiality protection SHOULD be provided if necessary.
- All feasible deployment scenarios, along with the relevant authentication/authorization models must be considered.

## 4. Non-Goals

This following issues are clearly outside the scope of bootstrapping:

- Home prefix renumbering is not explicity supported as part of bootstrapping. If the MN executes the bootstrap procedures everytime it powers-on (as opposed to caching state information from previous bootstrap process), then home network renumbering is taken care of automatically.

- Bootstrapping in the absence of a trust relationship between MN and any provider, is not considered. The reason for this is described in Section 9.

# 5. Motivation for bootstrapping

## 5.1 Addressing

The default bootstrapping described in the Mobile IPv6 base specification [2] has a tight binding to the home addresses and home agent addresses.

In this section, we discuss the problems caused by the currently tight binding to home addresses and home agent addresses.

### 5.1.1 Dynamic Home Address Assignment

While it is possible for the home address to be dynamically assigned, the HA cannot verify that the MN is authorized to use a particular address. As a result, static home address assignment is really the only home address configuration technique compatible with the current specification.

However, support for dynamic home address assignment would be desirable for the following reasons:

DHCP-based address assignment

Some ASPs may want to use DHCPv6 from the home network to configure home addresses.

Recovery from a duplicate address collision

It may be necessary to recover from a collision of addresses on the home network.

Addressing privacy

It may be desirable to establish randomly generated addresses as in RFC 3041 and use them for a short period of time. Unfortunately, current protocols make it possible to use such addresses only from the visited network. As a result, these addresses can not be used for communications lasting longer than the attachment to a particular visited network.

Ease of deployment

In order to make deployment of Mobile IPv6 easy, it would be desirable to free users and administrators from the task of allocating home addresses and specifying them in the security policy database.

This is consistent with the general IPv6 design goal of using autoconfiguration whereever possible.

Prefix changes in the home network

The Mobile IPv6 specification contains support for a mobile node to autoconfigure a home address based on its discovery of prefix information on the home subnet [2]. Autoconfiguration in case of network renumbering is done by replacing the existing network prefix with the new network prefix.

Subsequently, the MN needs to update the mobility binding in the HA to register the newly configured Home Address. However, the MN may not be able to register the newly configured address with the HA if a security association related to that reconfigured Home Address does not exist in the MN and the HA. This situation is not handled in the current MIPv6 specification [2].

### 5.1.2 Dynamic Home Agent Assignment

Currently, the address of the home agent is specified in the security policy database. Support for multiple home agents requires the configuration of multiple security policy database entries.

However, support for dynamic home agent assignment would be desirable for the following reasons:

Home agent discovery

The Mobile IPv6 specification contains support for a mobile node to autoconfigure a home agent address based on a discovery protocol [2].

Independent network management

An ASP may want to dynamically assign home agents in different subnets, that is, not require that a roaming mobile node have a fixed home subnet.

Local home agents

The mobile node's home ASP may want to allow a local roaming partner ASP to assign a local home agent for the mobile node. This is useful both from the point of view of communications efficiency, and has also been mentioned as one approach to support location privacy.

Ease of deployment

MSP may want to allow "opportunistic" discovery and utilization of its mobility services without any prearranged contact. These scenarios will require dynamic home address assignment.

### 5.1.3 Management requirements

As described earlier, new addresses invalidate configured security policy databases and authorization tables. Regardless of the specific protocols used, there is a need for either an automatic system for updating the security policy entries, or manual configuration. These requirements apply to both home agents and mobile nodes, but it can not be expected that mobile node users are capable of performing the required tasks.

## 5.2 Security Infrastructure

### 5.2.1 Integration with AAA Infrastructure

The current IKEv1-based dynamic key exchange protocol described in [3] has no integration with backend authentication, authorization and accounting techniques unless the authentication credentials and trust relationships use certificates or pre-shared secrets.

Using certificates may require the ASP to deploy a PKI, which may not be possible or desirable in certain circumstances. Where a traditional AAA infrastructure is used, the home agent is not able to leverage authentication and authorization information established between the mobile node, the foreign AAA server, and the home AAA server when the mobile node gains access to the foreign network, in order to authenticate the mobile node's identity and determine if the mobile node is authorized for mobility service.

The lack of connection to the AAA infrastructure also means the home agent does not know where to issue accounting records at appropriate times during the mobile node's session, as determined by the business relationship between the home ASP and the mobile node's owner.

Presumably, some backend AAA protocol between the home agent and home AAA could be utilized, but IKEv1 does not contain support for exchanging full AAA credentials with the mobile node. It is worthwhile to note that IKEv2 provides this feature.

### 5.2.2 Opportunistic or Local Discovery

The home agent discovery protocol does not support an "opportunistic" or local discovery mechanisms in an ASP's local access network. It is expected that the mobile node must know the prefix of the home subnet in order to be able to discover a home agent. It must either obtain that information through prefix update or have it statically configured. A more typical pattern for interdomain service discovery in the Internet is that the client (mobile node in this case) knows the domain name of the service, and uses DNS in some manner to find the server in the other domain. For local service discovery, DHCP is typically used.

## 5.3 Topology Change

### 5.3.1 Dormant Mode Mobile Nodes

The description of the protocol to push prefix information to mobile nodes in Section 10.6 in [2] has an implicit assumption that the mobile node is active and taking IP traffic. In fact, many, if not most, mobile devices will be in a low power "dormant mode" to save battery power, or even switched off, so they will miss any propagation of prefix information. As a practical matter, if this protocol is used, an ASP will need to keep the old prefix around and handle any queries to the old home agent anycast address on the old subnet, whereby the mobile node asks for a new home agent as described in Section 11.4, until all mobile nodes are accounted for. Even then, since some mobile nodes are likely to be turned off for long periods, some owners would need to be contacted by other means, reducing the utility of the protocol.

Bootstrapping does not explicitly try to solve this problem of home network renumbering when MN is in dormant mode. If the MN can configure itself after it 'comes back on' by reinitiating the bootstrapping process, then network renumbering problem is fixed as a side-effect.

## 6. Network Access and Mobility services

This section defines some terms as it pertains to authentication and practical network deployment/roaming scenarios. This description lays the ground work for Section 7. The focus is on the 'service' model since, ultimately, it is the provider providing the service that wants to authenticate the mobile (and vice-versa for mutual authentication between provider and the user of the service).

Network access service enables a host to send and receive IP packets on the Internet or an intranet. IP address configuration and IP packet forwarding capabilities are required to deliver this service. A network operator providing this service is called an access service provider (ASP). An ASP can be a commercial ASP, the IT department of an enterprise network, or the maintainer of a home (residential) network.

When the network service requires authentication, the concept of home ASP and serving ASP comes into the picture. Home ASP is the provider with whom the user has an account. Therefore, when the user directly connects to the home ASP network, the ASP can perform authentication without relying on any other service provider. On the other hand, when the user is roaming on the Internet, it may connect to another ASP network that has a roaming agreement with the home ASP. That ASP is called serving ASP. The serving ASP cannot authenticate a roaming user on its own, for that it needs to contact the home ASP.

A host does not always have to use an IP address from one of its home ASP prefixes. It may be configured with one from the serving ASP's prefixes. In fact, the home ASP may not even have a physical access network, in which case it could be identified as a virtual operator.

Another service is called Mobile IPv6 service, which enables a host to maintain its IP reachability despite changing its network attachment points (subnets). Providing Mobile IPv6 service involves setting up a home agent on a subnet that acts as a Mobile IPv6 home link. Home agent's responsibility include tunneling host's IP packets between the home link and its current point-of attachment. A network operator providing this service is called a mobility service provider (MSP). Mobile IPv6 requires authentication between the host and the home agent. The MSP that maintains an account for the user is called a home MSP. A home MSP can authenticate its users without relying on any other service provider. Conceptually, the user may be receiving the Mobile IP service from another MSP that has a roaming agreement with the home MSP. Such a service provider is called serving MSP. A serving MSP needs to contact the home MSP in order to authenticate the user before providing the mobility service.

A host may authenticate with a MSP based on the some kind of AAA association with the ASP (typically the home ASP or through the home ASP).

A host does not always have to use a Mobile IPv6 home address from one of its home MSP prefixes. It may be configured with one from the serving MSP's prefixes. In fact, the home MSP may not even have a physical access network, in which case it could be identified as a virtual operator.

Network access and Mobile IPv6 are two distinct services. A host can choose to have only network access service, or both network access and Mobile IPv6 services at the same time. Only having Mobile IPv6 service is not possible, since the Mobile IPv6 protocol requires ability to send and receive IPv6 packets. Even when both services are received by a host, the service providers involved might vary. All combinations are possible with respect to the choice of ASPs and MSPs:

- The serving ASP might be the home ASP. Similarly, the serving MSP might be the home MSP.
- The home ASP and the home MSP may be the same operator, or not. When they are the same, the same set of credentials may be used for both services.
- The serving ASP and the serving MSP may be the same operator, or not.
- It is possible that serving ASP and home MSP are the same operator.

Similarly the home ASP and serving MSP may be the same.

These entities and possible combinations must be taken into consideration when solving the Mobile IPv6 bootstraping problem. They impact home agent discovery, home address configuration, and mobile node to home agent authentication aspects.

## 7. Deployment scenarios

This section describes the various network deployment scenarios. The various combinations of service providers as described in Section 6 are considered.

For each scenario, the underlying assumptions are described. The basic assumption is that there is a trust relationship between mobile user and the MSP. Typically, this trust relationship is between the mobile user and AAA in the MSP network. Seed information needed to bootstrap the mobile node is considered in two cases (i) AAA authentication is mandatory for network access "&amp" (ii) AAA authentication is not part of network access. The seed information is described further in Section 8.

### 7.1 Mobility Service Subscription Scenario

Many commercial deployments are based on the assumption that mobile nodes have a subscription with a service provider. In particular, in this scenario the MN has a subscription with an MSP, called the home MSP, for Mobile IPv6 service. As stated in Section 6, the MSP is responsible of setting up a home agent on a subnet that acts as a Mobile IPv6 home link. As a consequence, the home MSP should explicitly authorize and control the whole bootstrapping procedure.

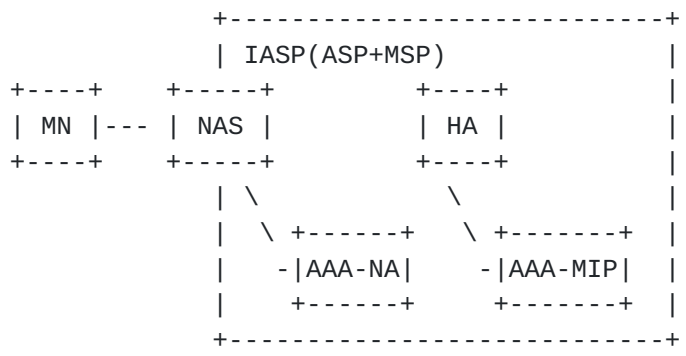
Since the MN is assumed to have a pre-established trust relationship with its home provider, it must be configured with an identity and credentials, for instance an NAI and a shared secret by some out-of-band means before bootstrapping, for example by manual configuration.

In order to guarantee ubiquitous service, the MN should be able to bootstrap MIPv6 operations with its home MSP from any possible access location, such as an open network or a network managed by an ASP, that may be different from the MSP and may not have any pre-established trust relationship with it.

### 7.2 Integrated ASP network scenario

In this scenario, the ASP and MSP are the same ASP. MN shares security credentials for access to the network and these credentials can be used to bootstrap MIPv6. This bootstrapping can be done during the same phase as access authentication/authorization or at a later time (probably based on some state created during access authentication/authorization).

Figure 1 describes an example AAA design for integrated ASP scenario.




NAS: Network Access Server
AAA-NA: AAA for network access
AAA-MIP: AAA for Mobile IP service

Figure 1: Integrated ASP network

## 7.3 Third party MSP scenario

Mobility service has traditionally been provided by the same entity that authenticates and authorizes the subscriber for network access. This is certainly the only model supported by the base Mobile IPv6 specification.

In the 3rd party mobility service provider scenario, the subscription for mobility service is made with one entity (home MSP for instance a corporate network), but the actual mobility service is provided by yet another entity (such as an operator specializing on this service, the serving MSP). These two entities have a trust relationship. Transitive trust among the mobile node and these two entities may be used to assure the participants that they are dealing with, are trustworthy peers.

This arrangement is similar to the visited - home operator roaming arrangement for network access.

Figure 2 describes an example network for third party MSP scenario.

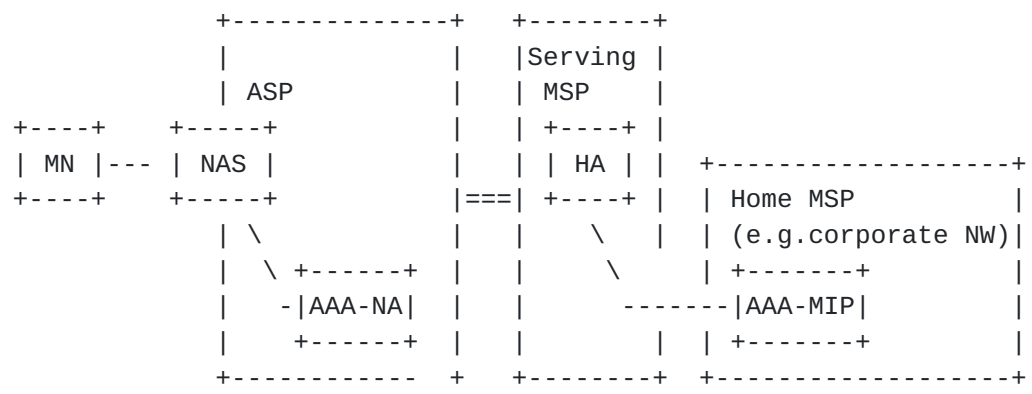



Figure 2: Third Party MSP network

## 7.4 Infrastructure-less scenario

Infrastructure refers to network entities like AAA, PKI, HLR etc. Infrastructure-less implies that there is no dependency on any elements in the network with which the user has any form of trust relationship.

In such a scenario, there is absolutely no relationship between host and infrastructure.

A good example of infrastructure-less environment for MIP6 bootstrapping is the IETF network at IETF meetings. It is possible that there could be MIP6 service available on this network (i.e a MIPv6 HA). However there is not really any AAA infrastructure or for that matter any trust relationship that a user attending the meeting has with any entity in the network.

This specific scenario is not supported in this document. The reason for this is described in Section 9.

## 8. Parameters for authentication

The following is a list of parameters that are used as the seed for the bootstrapping procedure. The parameters vary depending on whether authentication for network access is independent of authentication for mobility services or not. Authentication for network access is always independent of authentication for mobility services if different client identities are used for network access and mobility services.

- Parameter Set 1

  In this case, authentication for network access is independent of authentication for mobility services.

  If the home agent address is not known to the mobile node the following parameter is needed for discovering the home agent address:

  * The domain name or FQDN of the home agent

  This parameter may be derived in various ways such as (but not limited to) static configuration, use of the domain name from the network access NAI (even if AAA for network access is not otherwise used) or use of the domain name of the serving ASP where the domain name may be obtained via DHCP in the serving ASP.

  If the home agent address is not known but the home subnet prefix is known, Dynamic Home Agent Address Discovery of Mobile IPv6 may be used for discovering the home agent address and the above parameter may not be used.

  When the home agent address is known to the mobile node, the following parameter is needed for performing mutual authentication between the mobile node and the home agent by using IKE:

  * IKE credentials(*)

  In the case where the home agent does not have the entire set of IKE credentials, the home agent may communicate with another entity (e.g., a AAA server) to perform mutual authentication in IKE. In such a case, the IKE credentials include the credentials used between the mobile node and the other entity. In the case where a AAA protocol is used for the communication between the home agent and the other entity during the IKE procedure, AAA for Mobile IPv6 service may be involved in IKE.

- Parameter Set 2

  In this case, some dependency exists between authentication for network access and authentication for mobility services in that a security association that is established as a result of authentication for network access is re-used for authentication for mobility services.

  All required information including IKE credentials are bootstrapped from the following parameter:

  * Network access credentials(*)

(*) A pair of a NAI and a pre-shared secret is an example set of credentials. A pair of an NAI and a public key, which may be provided as a digital certificate, is another example set of credentials.

## 9. Security Considerations

The bootstrapping procedure needs to create a security association that matches the requirements set for its use. Mobile IPv6 base specification expects strong, mutual authentication and trust relationship between the mobile node and home agent. This is necessary, for instance, to ensure that fraudulent mobile nodes that flood other nodes with traffic [draft-ietf-mipv6-ro-sec] can not only be shut off from the service, but also tracked down. The use of infrastructureless techniques does not satisfy these requirements, at least not without introducing additional routability tests to the Mobile IPv6 home registration procedure.

Thus, the case of infrastructure-less network where there is absolutely no pre-mediated trust is kept outside of scope of this document.

Another requirement is that the "ownership" to a particular home address must be authorized to at most one mobile node at a time. This implies that a Mobile IPv6 security association is always tied to zero or more such authorizations; these authorizations can either be created at the time the security association is created, or dynamically managed through, for instance, a First Come First Served allocation policy.

Where an automatic bootstrap process is used, it becomes necessary to associate a lifetime with all the parameters which are bootstrapped. Otherwise a large number of unused security associations would have to be stored by the participating nodes, either by accident or through malicious behaviour or the mobile node will have stale information.

The specific mean of verifying the security association is not defined in this document, but it can be, for example a set of IKE credentials, an IPsec security association, a username-password -like association or digital signature constructed by a certified key.

The bootstrap process itself may have vulnerabilities. The following issues need to be addressed:

- Mutual authentication and trust relationship between the mobile node and the entity handling the bootstrap process. Refer to Section 7.15 in [9] and [10] for further information.
- Cryptographic separation and naming of session keys used for multiple purposes, such as network access authentication and mobility service.
- Ensuring that key lifetimes are not exceeded.

- Binding security associations to specific home agent and address allocations.
- Support of multiple algorithms for the resulting security associations.
- Avoidance of denial-of-service vulnerabilities.

## 10. Contributors

This contribution is a joint effort of the problem statement design team of the Mobile IPv6 WG. The contributors (alphabetical order) include Jari Arkko, Samita Chakrabarti, Kuntal Chowdhury, Vijay Devarapalli, Gopal Dommety, Gerardo Giaretta, James Kempf, Kent Leung, Yoshihiro Ohba, Hiroyuki Ohnishi, Basavaraj Patil, Hannes Tschofenig, Ryuji Wakikawa, Mayumi Yanagiya and Alper Yegin.

## 11. Acknowledgments

Special thanks to James Kempf and Jari Arkko for writing the initial version of the bootstrapping statement.

# 12. References

## 12.1 Normative References

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

[2] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, July 2003.

[3] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", RFC 3776, July 2003.

[4] Manner, J. and M. Kojo, "Mobility Related Terminology", draft-ietf-seamoby-mobility-terminology-06 (work in progress), February 2004.

## 12.2 Informative References

[5] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-00 (work in progress), February 2004.

[6] Kempf, J. and J. Arkko, "The Mobile IPv6 Bootstrapping Problem", draft-kempf-mip6-bootstrap-00 (work in progress), March 2004.

[7] Patel, A., Leung, K., Akthar, H., Khalil, M. and K. Chowdhury, "Network Access Identifier Option for Mobile IPv6", draft-ietf-mip6-nai-option-00 (work in progress), February 2004.

[8] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

[9] Levkowetz, Ed., H., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-09 (work in progress), February 2004.

[10] Mariblanca, D., "EAP lower layer attributes for AAA protocols", draft-mariblanca-aaa-eap-lla-00.txt (work in progress), May 2004.

[11] Yegin, A., "AAA Mobile IPv6 Application Framework", draft-yegin-mip6-aaa-fwk-00 (work in progress), August 2004.

Author's Address

Alpesh Patel
cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408 853 9580
EMail: alpesh@cisco.com

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

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