

# ENABLING MOBILE IPV6 IN OPERATIONAL ENVIRONMENTS

Xiaoming Fu

*University of Göttingen*  
*fu@cs.uni-goettingen.de*

Hannes Tschofenig,  
Srinath Thiruvengadam

*Siemens AG*  
*{hannes.tschofenig,*  
*srinath.thiruvengadam}@*  
*@siemens.com*

Wenbing Yao

*Brunel University*  
*wenbing.yao@brunel.ac.uk*

**Abstract:** Although Mobile IPv6 allows maintaining transport layer connections alive when an IPv6 node roams to different access networks, certain enabling mechanisms are needed for it to work in large scale network scenarios, including, most notably, issues with Mobile IPv6 bootstrapping and firewall traversal. This paper tries to address these problems by extending the IETF PANA and NSIS protocols to form an extensible framework for wide deployment of a secure, light-weight mobility service in operational IPv6 environments.

## 1. Introduction

With the recent tremendous penetration of the Internet technology and numerous portable devices, a number of new demands march steadily into view. Among them, two problems needed immediate attention: the insufficient IPv4 addresses and the need for mobility support in IP-based networks. The next generation Internet protocol (IPv6) intends to satisfy these needs. In its mobility support protocol (MIPv6) [5], the node's locator is somewhat separated from the identifier, by introducing a fixed Home Address (HoA) for each mobile node (MN) in addition to its topologically reachable address, the Care of Address (CoA). When the MN is away from its home network, a router on the same link as this address (the Home Agent, HA) redirects any traffic from a corresponding node (CN) to the MN's HoA to its current CoA. Due to its intrinsic mobility support for IPv6, MIPv6 has been regarded as an indispensable component of the next generation Internet infrastructure. However, MIPv6 itself simply describes a signaling protocol which establishes tunnels to change the routing of IP packets and requires pre-configured HoA information, security associations or SAs (e.g., for authentication of the MN and for MIP signaling protection), and assumes there is no firewall or other middleboxes. However, any inability to fulfill these assumptions in a foreseen scenario can cause a number of subsequent problems.

These problems can be broadly grouped into two categories: a lack of MIPv6 bootstrapping mechanisms [7] or a lack of middlebox traversal mechanisms [6]. In this paper we advocate a new approach to address them: bootstrapping is done by extending the IETF Protocol for carrying Authentication for Network Access (PANA) [3], whereas middlebox states are dynamically configured to allow MIPv6 packets to traverse by extending the IETF NSIS NAT/Firewall signaling protocol (NATFW NSLP) [10]. Eventually, control data required for MIPv6 operation can be obtained and their runtime utilization (such as encapsulation of data packets and routing according to binding information, viewed as the data plane function), would be achieved seamlessly, thus forming a universal mobile IPv6 operational framework.

## 2. Mobile IPv6 Bootstrapping

During the MIPv6 initialization phase i.e., when an MN is started in home network or moves to (or is restarted in) a foreign network, some problems may arise, e.g., the node cannot obtain enough information for MIPv6 to work or lacks support for working with the infrastructure (such as AAA). They are identified as bootstrapping functions according to the IETF MIP6 working group [7]. By and large, we can categorize them into two groups:

- a. Functions related to the acquisition of parameters by the MN for the MN-HA communication. These include HoA, HA address and the parameters required for IPsec security association (SA) setup between MN and the HA.
- b. Functions related to MN's interaction with the access network, e.g., regarding the MN-AAA policy enforcement point (PEP) or MN-firewall device relationships for run-time control or forwarding. These include e.g., authentication of the MN and key exchange with the firewall device.

Basically, 2 approaches for addressing these issues are conceivable: 1) to address them individually using different, dedicated mechanisms and then combine them in a single system; or 2) to use a more extensible method based on which various bootstrapping issues are addressed, allowing the flexibility to enable certain features. Obviously, the first approach suffers from interworking and extensibility concerns. By contrast, the second one provides more flexibility for (potentially light-weight) bootstrapping mechanisms design.

Unfortunately, most proposals follow the first approach and just limit to certain functions. For example, the IETF defined a dedicated method for MIPv6 authentication and MN-HA key exchange [2], while others suggest (e.g., [4]) to setup MN-HA IKE pre-shared secret based on existing protocols such as PANA or DIAMETER. In [12] we propose to focus on the SA establishment for the recently defined MIP6 authentication [7] based on PANA since PANA already

provides mechanisms to bootstrap an IKE pre-shared secret for the establishment of an IPsec SA. This approach, in its first form, also belongs to the first classification as described above. However, due to its additional ability to run PANA in a multi-hop environment, it relaxes PANA assumptions and hence resolves more general bootstrapping issues. Below we shortly review PANA, then present our extension and discuss how it addresses bootstrapping problems.

### ***2.1. Protocol for Carrying Authentication for Network Access***

PANA is a transport mechanism for the Extensible Authentication Protocol (EAP) [1] to enable network access authentication between clients and access networks. PANA carries EAP payload, allowing the use of many authentication methods. By enabling UDP transport of EAP, PANA allows any authentication method to be carried as an EAP method and hence neutral to any link-layer technology. PANA runs between the PANA client (PaC, an end node which uses PANA to authenticate itself to the network) and the PANA authentication agent (PAA, the endpoint of the PANA protocol at the access network) after successful PANA operation. A detailed description of PANA can be found in [3].

### ***2.2. Extensions to PANA for MIPv6 bootstrapping***

We assume that the MN acts as a PaC and some agent in the network (most likely the HA) acts as the PAA (which can be co-located with the PEP, or even HA). Our approach requires PANA to traverse multiple PANA hops. After mutual authentication, the PaC SA will be established. Here is a summary how we extend PANA to address various MIPv6 bootstrapping issues:

#### **Home Agent Discovery**

PANA was designed with a focus on network access authentication and the PAA is assumed to be just one IP hop away from the PaC. Thus, in its discovery mechanism, a multicast address is used as the discovery message's destination [3]. Here, we extend the PANA discovery mechanism to be able to directly address the PAA using the PAA's unicast address (if it knows this), or (indirectly) a multicast address with the router alert option (RAO) enabled. Such messages are ignored and forwarded further on by routers, until received by a PAA. Once the PAA detects the discovery message with RAO, it responds to the PaC with PANA-start/-answer message including HA's information. Whenever possible, the MN can also learn about the HA by simpler means, such as manual configuration, DNS or IPv6 anycast mechanism.

#### **Obtaining Home Address**

The payload of a PANA message consists of zero or more Attribute Value Pairs

(AVP). We propose a new AVP (HoA AVP) for carrying the MN's HoA; pre-configuring HoA in the MN is not required. Upon receipt of a PANA request in the PAA, the HoA is selected either randomly or based on user authentication, and placed into the HoA AVP which is integrity protected by PANA.

#### **Security Association Establishment**

An SA, so-called MIPv6 SA, is required for subsequent protection of MIPv6 MN-HA signaling messages. It involves at least the following parameters as part of the bootstrapping procedure [7]: Security Parameter Index (SPI), replay protection indicator (e.g., timestamp or sequence number) and cryptographic algorithms. We extend PANA with a new AVP for negotiation of these parameters. Additionally, a session key needs to be derived for the MIPv6 SA. For this purpose we propose to reuse the session key derivation procedure as defined in the PANA SA establishment based on the EAP method [3]. When necessary, use of PANA re-authentication [3] also allows re-keying of SAs (including the PANA SA and the MIPv6 SA).

A further issue here is how the MIPv6 SA state should be maintained, which can impact the scalability and robustness of the bootstrapping mechanism. In principle the state lifetime can be either negotiated (e.g., the PaC proposes a value and the PAA either accepts or modifies it), fully dictated by the MN's home network, or short-lived (which requires periodical refreshes). The short-lived approach additionally deals with failure detection and prevents leaving orphan state at the home agent for a long time. This seems more interesting also because PANA already provides a refresh mechanism.

### **3. Middlebox Traversal in Mobile IPv6**

MIPv6 does not cope with firewalls and other middleboxes. For example, if a CN is located behind a firewall, there needs to be a mechanism to allow MIPv6 signaling messages (and data traffic) to traverse it successfully. We propose a new solution based on the IETF NSIS protocol for middlebox state maintenance.

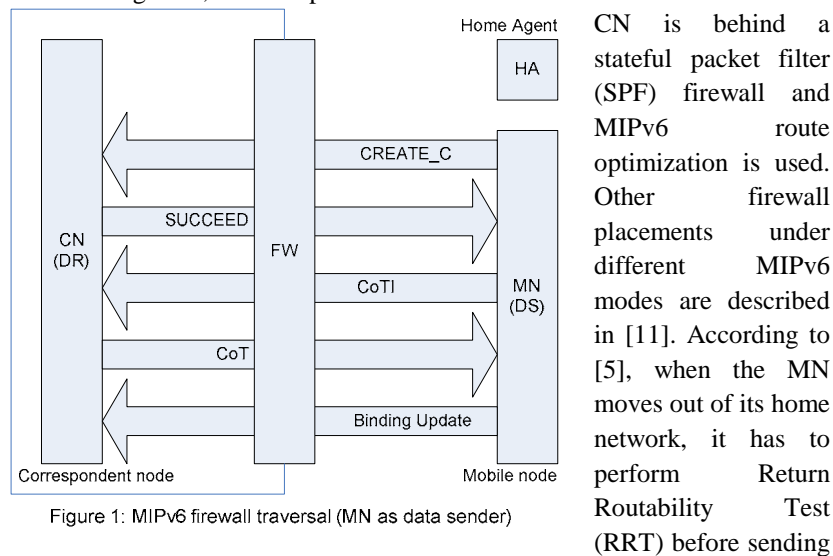
#### **3.1. NSIS NAT/Firewall Signaling**

The IETF NSIS working group is specifying an extensible IP signaling transport protocol GIMPS [9], based on which several signaling application protocols are being developed; NATFW NSLP [10] is one of them. In addition to NAT bindings, the NATFW NSLP can install, manage and remove firewall states (pinholes) along the flow path, as follows: after a sender learns about the receiving node's IP address and port number (via higher layer e.g., SIP), it constructs a NATFW NSLP CREATE message which includes its flow

description and send it towards the data receiver (DR). Upon receipt, the firewall authenticates and authorizes the request, and installs the packet filter as specified in the flow identifier. From now on, data traffic will be allowed to traverse it.

### 3.2. Providing MIPv6 Firewall Traversal by NSIS Signaling

As shown in Figure 1, an example scenario is studied in this section where the



CN is behind a stateful packet filter (SPF) firewall and MIPv6 route optimization is used. Other firewall placements under different MIPv6 modes are described in [11]. According to [5], when the MN moves out of its home network, it has to perform Return Routability Test (RRT) before sending a binding update to the CN: it sends a HoTI message through the HA to the CN and awaits a HoT message from the CN; it also sends a CoTI message directly to the CN and awaits a CoT message from the CN. The SPF will only allow packets that belong to an existing session and hence both the packets (HoTI, CoTI) will be dropped as these packets are MIPv6-specific packets having a header structure different from normal IPv6 packets. Consequently, RRT fails. It is clear that packet filter rules have to be changed to allow these signaling messages (as well as data packets) to traverse.

The MN initiates the NSIS session by sending a CREATE to the CN. The FW may not need to know the MN, thus may not be able to authenticate the MN. It stores some relevant state regarding this firewall policy installation request and waits for the CN's authorization. Once the CN approves the request, the FW will install the relevant policy requested by the MN. When the MN receives both the messages CoT and HoT, it will construct the binding key and perform binding update to the CN. Note the signaling that was aforementioned was only to allow the MIPv6 signaling messages. If the MN wants to continue sending data traffic

(MN is the DS), it has to perform another round of signaling (with appropriate flow identifier) to install filter rules for data traffic. Enhancements to NATFW NSLP are necessary for use with MIPv6; more details are discussed in [12].

#### **4. An architecture for enabling MIPv6 deployment**

Although the aforementioned issues have been examined in some recent works, there is no clear architectural consideration for enabling MIPv6 in operational environments. In this section we propose a conceptual architecture that covers (but not limited to) MIPv6 bootstrapping and firewall traversal. It defines the enabling mechanisms through 3 planes of functionalities, namely the management, control and data planes. The management plane involves MIPv6 RRT and bootstrapping mechanisms. The control plane manages control state information for MIPv6 message exchange and data forwarding, including functionalities for MIPv6 registration and middlebox signaling. The data plane uses IP encapsulation and forwarding to handle data traffic.

First, the bootstrapping procedure will be initiated to set up security associations for MIPv6. Once the bootstrapping is completed, MIPv6 signaling can start. Since the MN, the CN and the HA could be behind firewalls or other middleboxes, middlebox need to be configured and maintained to allow MIPv6 messages, where NSIS signaling can be used.

Without architectural impacts, either IPsec or the MIP6 authentication protocol can be used to protect MIPv6 signaling messages. Other components which perform bootstrapping (especially to establish the MN-HA SAs) are based on the PANA extension described in Section 3. Under this architecture, it is easy to develop further necessary mechanisms for enabling successful MIPv6 operation. For example, if certain parameters are required for the control plane, the management plane functionality needs to assist and prepare them in prior to the control plane operation. One realistic example is that in most cases, NSIS signaling for middlebox traversal (a control plane function) requires security association between the MN and a middlebox device, before starting NSIS signaling. Here, PANA-based bootstrapping (a management plane function) can be easily extended for such purposes.

Figure 2 shows such an approach where PANA is used to perform both MIPv6 bootstrapping and NSIS bootstrapping. When the MN is successfully authorized, it receives a response in the PANA messages which makes a token available to the NSIS protocol. When authorization is needed, this token is added to the NSIS signaling authorization procedure.

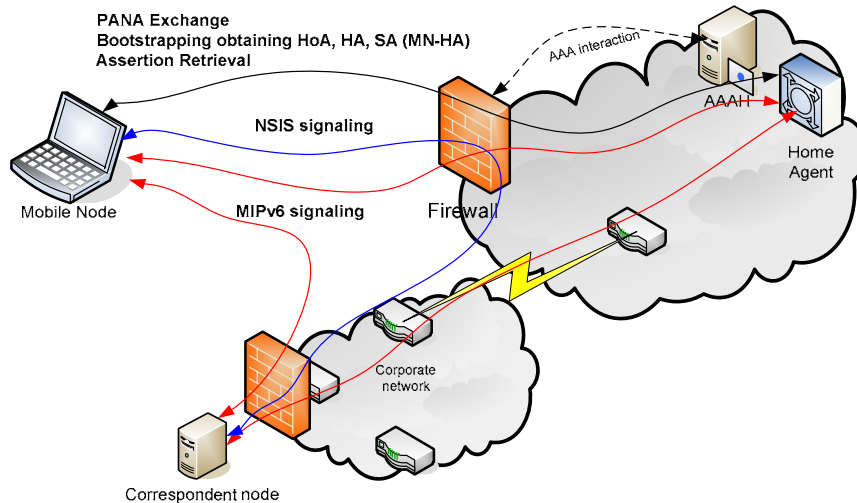


Figure 2: An example of MIPv6 in operational environments

Several aspects need to be noted with this approach. After finishing the MIPv6 bootstrapping procedure, MIPv6 related information (including keying material) can be sent to the HA (push approach). PANA can be executed either directly with the HA or with another entity, since the PANA framework supports decoupling of the enforcement point (in this case the HA) and the PAA. The latter method can be utilized by a load balancing approach. With NATFW-NSLP signaling a pull approach can work even better since the traversed firewall is unknown to the MN in advance. Note that pushing security information may not be possible in more complex topologies with multiple middleboxes and routing asymmetry, which might result in the signaling exchange towards the HA encounters an unexpected firewall. With a push approach, when the NSIS signaling message arrives at one of the firewalls, it can contact the AAA server for authentication and authorization and fetching the security context.

## 5. Summary and Future Work

In order to successfully enable MIPv6 technology, there are a number of challenges to be addressed. We have chosen two of the most prominent ones: MIPv6 bootstrapping and firewall traversal for investigation and proposed to extend PANA in the management plane and NSIS signaling in the control plane in coordination with the data plane. We believe such a unified, extensible enabling architecture can enhance MIPv6 with envisioned enabling facilities and meet emerging new requirements. Nevertheless this work needs further

investigation, including detailed message flows in different scenarios, tradeoffs between performance and complexity, and support for other features (such as VPNs). We are working on implementations of the NSIS protocol suite (including NATFW-NSLP) and PANA, and plan to integrate them into the proposed architecture and to evaluate the performance and the scalability.

### Acknowledgments

We would like to thank members of the IETF MIP6, PANA and NSIS working groups for the fruitful discussions. In particular we would like to thank Frank Le, Yoshi Ohba, Alper Yegin, Dan Forsberg, Gerardo Giaretta, Julien Bournelle, Antonio Gomez-Skarmeta and Rüdiger Geib.

### References

1. Aboba, B., Blunk, L. and *et al.*, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
2. Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.
3. Forsberg, D., Ohba, Y., and *et al.*, "Protocol for Carrying Authentication for Network Access (PANA)", Internet draft, work in progress, Oct 2004.
4. Jee, J., Nah, J. and K. Chung, "Diameter Mobile IPv6 Bootstrapping Application using PANA", Internet draft, work in progress, Oct 2004.
5. Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
6. Le, F., Faccia, S. and *et al.*, "Mobile IPv6 and Firewalls Problem Statement", Internet draft, work in progress, Oct 2004.
7. Patel, A., "Problem Statement for bootstrapping Mobile IPv6", Internet draft, work in progress, Oct 2004.
8. Patel, A., Leung, K. and *et al.*, "Authentication Protocol for Mobile IPv6", Internet draft, work in progress, Dec 2004.
9. Schulzrinne, H. and R. Hancock, "GIMPS: General Internet Messaging Protocol for Signaling", Internet draft, work in progress, Oct 2004.
10. Stiemerling, M., Tschofenig, H., and *et al.*, "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", Internet draft, work in progress, Oct 2004.
11. Thiruvengadam, S., Tschofenig, H. and F. Le, "Mobile IPv6 – NSIS Interaction for Firewall Traversal", Internet draft, work in progress, Oct 2004.
12. Tschofenig, H. and S. Thiruvengadam, "Bootstrapping Mobile IPv6 using PANA", Internet draft, work in progress, Oct 2004.