

# Mobile IP and the IETF

Charles E. Perkins

*charles.perkins@eng.sun.com*

SUN Microsystems, Mountain View, CA, USA

## Mobile Networking at IETF 45

Developments in the Mobile IP working group continue to proceed at a fairly rapid pace. One of the first orders of business at the recent IETF working group meeting in Oslo was to announce yet another change in the working group leadership. After his appointment to be Internet Area Director, Erik Nordmark has decided to step down as co-chair. Phil Roberts has been named to take over as co-chair with Basavaraj Patil. Erik continued the tradition of providing strong leadership to the `mobile-ip` working group during his tenure as co-chair, and this has been much appreciated. As always, contributions to the `mobile-ip` mailing list should be sent to *mobile-ip@standards.nortelnetworks.com*.

### I. Revised Mobile IP Charter

A revised Mobile IP working group charter has been accepted by the working group and the Area Directors. Prominent in the work items called out in the new charter is the interaction between Mobile IP and AAA (Authentication, Authorization, and Accounting) protocols. The new charter is expected to serve the needs of manufacturers of mobile telephony equipment, who are quite interested in incorporating IETF standard protocols into their products.

Here are the new charter milestones:

**Jun 99** Submit the Mobility Support in IPv6 to the IESG for consideration as a Proposed Standard.

**Jun 99** Submit Internet-Draft for NAI support in Mobile IP to IESG for consideration as a Proposed Standard.

**Aug 99** Review the use of AAA in Mobile IP to support inter-domain and intra-domain mobility and dynamic home agent assignment.

**Dec 99** Review security framework requirements for Mobile IP.

**Dec 99** Review solutions and submit drafts for mobility in private address spaces.

**Dec 99** Submit draft on using AAA in Mobile IP for inter-domain and intra-domain mobility as a proposed standard.

**Dec 99** Submit draft capturing cellular requirements to IESG as an Informational RFC.

**Jul 00** Review QoS in a Mobile IP enabled network.

**Jul 00** Submit Mobile IPv6 MIB to IESG for consideration as a Proposed Standard

**Sep 00** Submit the IPv4 Mobile IP Protocol to the IESG for consideration as a Draft Standard.

The NAI draft is basically finished, and should be sent for IETF last call soon; I believe the draft has finished working group last call. Mobile IPv6 standardization is discussed below in section II, and AAA status is detailed in section IV. There was a draft submitted about private addresses, and the discussion in the working group is summarized in section V. A new draft for cellular requirements was submitted in time for the Internet Draft deadline, but not discussed at the working group meeting. Not much work is under current discussion about QoS, but that may change as work progresses with differentiated services within the IETF.

### II. Mobile IPv6

The Mobile IPv6 draft is practically finished. The last unsettled point has to do with how to process outbound IPv6 security headers when the mobile node uses the Home Address destination option on outgoing packets. There is difficulty because the mobile node will use the care-of address as the source IP address, and yet (presumably) use the home address for interaction with IKE (Internet Key Exchange) when selecting the correct security association for creating the IPSec headers. It's all very technical and picky, and the difficulty arises from the fact that IPSec equates source IP address with identity, and the Home Address destination option starts to break that model. During the IETF meeting, Dave Johnson met with some engineers familiar with IPSec, IPng, and Mobile IP. It's not easy to find people with those qualifications, but an IETF meeting is an awfully good place to look. The outcome, I believe, was that Dave has the solution in hand now for this last horrid point.

The new draft submitted just before the Oslo meeting does not solve that problem, but it did make a few minor improvements from the earlier draft:

- Actual values are used for the protocol parameters, since those values have now been allocated by IANA.
- Added another bit to the Binding Update option, to allow the mobile node to tell its Home Agent that the mobile node is also a router.
- clarifications made and typos fixed and boilerplate updated.

### III. Security Extensions

There were several proposals for new security extensions for Mobile IP registration messages. Vipul Gupta made a presentation about his recent draft, "An Inline Security Parameter Extension for Mobile IP" [3]. This proposal specifies a way to transmit key information (perhaps especially, public key certificate information) for use in an immediately subsequent authentication extension. Thus, it can be used with any

of the three currently defined authentication extensions (MN-HA, MN-FA, or FA-HA), and presumably future authentication extensions also (e.g., MN-AAA, or Route Optimization). The new extension makes use of a Key ID field, that enables the following Key Value field to be interpreted correctly in any of several predefined ways, or according to preconfiguration between the interested protocol entities. It also relies on a particular value (TBD) for the SPI in the following authentication extension.

In a slightly different direction, Pete McCann presented a new extension for Mobile IP registration messages that would allow new features to be used in tunnels between the Home Agent and care-of address [5]. These new features include a variety of encryption and compression protocols. Up until now, there has not been much discussion about how to manage encryption of data to the mobile node; it has usually been assumed that encrypted data would be managed by way of IPSec and additional headers inserted in the tunneled packets to the care-of address. This transform extension would make the tunnel setup happen as an explicit part of the Mobile IP registration process, and thus be more efficient than other alternatives seem to be. Yet another draft from McCann et.al. suggests the use of DIAMETER [1] and ideas similar to those in [5] to establish security policy for tunnels between the home agent and the foreign agent. In this case, the presumption is that the mobility agents should provide privacy for data tunneled over the Internet, even when the mobile node cannot (for implementation reasons) take part in creating the needed security association. Thus, the foreign agent and the home agent offer a “value-added” privacy service to mobile nodes that may not be able to run IPSec protocols.

Taking the opposite viewpoint, Raj Patil and his co-authors discussed a model using standard IPSec mechanisms to provide security for Mobile IP. In their proposal, a new entity known as a MCMGF (Mobile Control Message Gateway Function) serves as a target for all Mobile IP control messages. The MCMGF in the home domain must have a security association with the MCMGF in the foreign domain for the security associations to work out. A method is also described for using the MCMGF to implement a virtual private network for the mobile nodes and the home network. A MCMGF may also borrow some of the function of the recently discussed AAA servers to use intermediate security brokers for creating security associations between the home domain and a foreign domain.

Ken Peirce presented a proposal developed to enable the use of RADIUS or DIAMETER with CHAP as the authentication method. This involves allowing the use of MD5 in “prefix-only” mode (preferred by RADIUS) instead of the “prefix+suffix” mode required by default in base Mobile IP. Their proposal is geared to use the proposed “MN-AAA” authentication extension, with either RADIUS or DIAMETER as the AAA server.

#### IV. AAA Working Group Interaction

A new draft describing the Mobile IP requirements for AAA service [2] has been created for consideration by the aaa working group and the mobile-ip working group. This draft uses the model presented before in this column, and repeated here

for convenience in figure IV.

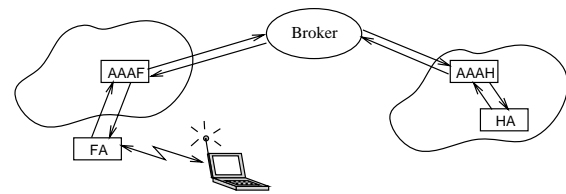


Figure 1: Mobile IP/AAA Framework

In the figure, the AAA servers take over the responsibility for authenticating the mobile node, and provide assurances to both the foreign agent and the home agent that the mobile node is authorized to access the connectivity resources in the foreign domain. The AAA servers are also expected to initiate accounting mechanisms as part of the Mobile IP registration sequence.

The requirements draft [2] presents this model for consideration by the aaa working group. Furthermore, it outlines quite a few detailed requirements that are to be placed on any future AAA protocol that would be developed within the AAA working group. The relationship between the model shown in figure IV and the detailed list of requirements is that the requirements are independent of the framework model, but that the model provides a good way to organize and understand a possible way to tie together a mechanism for meeting the requirements. This requirements draft needs a certain amount of refinement; the mobile-ip working group needs to make a clear determination about which features are absolute requirements for the aaa working group, and which features may be provided by more full-featured protocols.

One outcome of the aaa working group meeting was the general feeling that any standard AAA protocol would be years in the making. This does not fit well with the timeline envisioned in the mobile-ip working group. In fact, the TR45.6 group wants to have a AAA standard this year; unfortunately, this goal appears difficult to meet. I brought this topic up for discussion within the working group meeting on the last day of the IETF week, and a great deal of discussion took place about what might be done. I think that the sense of the working group is that we cannot wait for years. The first thing that the group decided to do was to produce an interface requirements document right away; the document could naturally be used by the aaa working group. But, more immediately, we could use the document to select from among a list of currently available AAA protocols to fulfill our requirements right away.

The roamops working group, also faced with the same dilemma of being unable to wait for the aaa working group to finish, decided almost unanimously to pursue the standardization of a particular AAA protocol (DIAMETER [1]). If the roamops charter modification is allowed to take effect by approval of the Area Directors, then it would be very convenient for the mobile-ip working group to use the results of the roamops working group’s efforts.

#### V. Private Addresses

The requirements documents from mobile telephone equipment manufacturers point out the need for Mobile IP to han-

dle private addresses – in other words, addresses that are not routable from the global Internet infrastructure. Such addresses are often allocated as needed in an enterprise intranet, without regard for any future direct connectivity to the global Internet. Because of the uncoordinated, distributed nature of this allocation strategy, it may well be the case that the same address is assigned to more than one mobile node. Furthermore, it is possible that several mobile nodes with the same private address may simultaneously enter the range of a foreign agent. The current definition for Mobile IP registration specified in RFC 2002 [10] does not enable that foreign agent to correctly distinguish registrations for such mobile nodes.

The main difficulty is in disambiguating the destination mobile node after the foreign agent decapsulates tunneled packets from the various home agents sending traffic to the mobile nodes. Given current routing practice, the foreign agent would not be able to tell which mobile node was which if several mobile nodes had the same IP address, because routing typically uses the IP address of the destination to make decisions about outgoing network interface selection and layer-2 addressing. So, if the encapsulation method is IP-within-IP [7], or Minimal Encapsulation [8], the foreign agent needs more information. It turns out that GRE [4] can give the foreign agent additional help by using the Key field as a tunnel identifier. But, to make use of the default standard encapsulation methods for private addresses, new procedures will be required. Some initial ideas are presented in a our new draft [9].

Unfortunately, it seems that the new draft does not handle all known cases very well. Researchers Wee-Tuck Teo and Y.C. Tay from University of Singapore have identified some unusual but perfectly legitimate cases that may cause difficulties. During the working group meeting in Oslo, it was suggested that mobile nodes be disallowed from using private addresses unless they can also obtain and manage colocated care-of addresses; in other words, unless they can do without foreign agents. This has the benefit of simplicity, and of actually working. However, this strategy also has the disadvantage of requiring a much larger pool of IP addresses for use of the mobile nodes.

## VI. Miscellaneous

Karim El Malki (University of Sheffield) made an interesting presentation about how to do fast handoffs. In his application, TCP disruptions on the order of 2.6-7.3 seconds were observed because of handoff problems. The smaller disruptions were achieved using Eager Cell Switching; I was surprised to see that there was any disruption in their setup, but it was caused in part by network traversal times. They propose a way for a mobile node to receive transmissions from multiple base stations (geared towards CDMA links), and they further propose the use of regional registrations within a hierarchy of foreign agents. As a related matter, many other people expressed support for such a regional registration scheme. Along with researchers from Ericsson Research, I have put together a draft for regional registration. There is also another draft available from Helsinki University of Technology about hierarchical foreign agents. This looks like another area of increasing technical interest.

Bob Heile discussed IEEE 802.15 and the standardization

effort for Wireless Personal Area Networks. He made the observation that IEEE is now more interested in timely standards than in perfect standards. Too bad we can't have both! The IEEE is seriously interested in maintaining liaison relationships with working groups in other standards bodies (e.g., IETF). Further information is available from the web (from the minutes):

### WPAN Archives

<http://grouper.ieee.org/groups/802/15>

### WPAN Mailing List

[stds-802-wpan@majordomo.ieee.org](mailto:stds-802-wpan@majordomo.ieee.org)

### IEEE 802.11

<http://grouper.ieee.org/groups/802/11>

### Bluetooth Special Interest Group

<http://www.bluetooth.com>

### Home RF Working Group

<http://www.homerf.org/>

Erik Nordmark made a detailed presentation about ways to handle IPv6 site-local addresses with Mobile IP. He proposes that mobile nodes can get site-local addresses for their communications peers from DNS, but that they have to ignore these site-local addresses unless the mobile nodes are confident that they are in the same site as the peer. This is accomplished by including new prefix length information in the Prefix Information Option from Neighbor Discovery [6], and by requiring each node to keep track of a list of site prefixes.

Ram Ramjee made an update on HAWAII, which is now even more transparent to mobile nodes running base Mobile IP. He also tried to describem, in an amount of time which was unfortunately too small, his recent efforts to incorporate paging into HAWAII.

Emad Quaddoura presented a proposal from Nortel aimed at eliminating a situation encountered while using the method of *smooth handoff* specified in the Route Optimization draft. The problem is that, in some circumstances, a mobile node may not wish an unauthorized foreign agent to have access to data being forwarded from the mobile node's previous foreign agent. However, the mobile node may instead wish it's previous foreign agent to begin buffering packets destined for the mobile node, for delivery when the new registration request is finished.

Other proposals were also presented, but it would not be possible to describe all of them in this short report.

## Conclusion

Mobile IP has entered a significant growth phase, and efforts from many interested groups are helping shape the future of the protocol. Discussion about AAA interactions are the most prominent among the several areas of current interest. Other areas of discussion include private addresses, route optimization, security context establishment, and mobility for IPv6 along with consideration for use of IPv6 site-local addresses. A number of new documents have been produced for consideration by the working group. The Mobile Node NAI extension

has completed working group last call, and should have completed IETF last call by the time this report is published.

As I write this, an interoperability test for Mobile IP and NAI, along with some other new features is underway during the week of July 26. In the next installment of this column, I will report on the results of the week's test.

## References

- [1] P. Calhoun and A. Rubens, "DIAMETER Base Protocol," draft-calhoun-diameter-07.txt, Nov. 1998. (work in progress).
- [2] S. Glass and S. J. et.al, "Mobile IP Authentication, Authorization, and Accounting Requirements," draft-ietf-aaa-mobile-ip-req-00.txt, June 1999. (work in progress).
- [3] V. Gupta, "Inline security parameter payload for mobile IP," draft-gupta-mobileip-inline-secparams-00.txt, June 1999. (work in progress).
- [4] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic Routing Encapsulation over IPv4 networks," RFC 1702, Oct. 1994.
- [5] P. McCann and T. Hiller, "IP transform policy distribution using mobile IP/DIAMETER," draft-mccann-transform-00.txt, June 1999. (work in progress).
- [6] T. Narten, E. Nordmark, and W. Simpson, "RFC 2461: Neighbor discovery for IP Version 6 (IPv6)," Dec. 1998, Status: DRAFT STANDARD.
- [7] C. Perkins, "IP Encapsulation within IP," RFC 2003, May 1996.
- [8] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, May 1996.
- [9] C. E. Perkins, G. Montenegro, and P. R. Calhoun, "Private addresses in mobile IP," draft-ietf-mobileip-privaddr-00.txt, June 1999. (work in progress).
- [10] C. Perkins, Editor, "IP Mobility Support," RFC 2002, Oct. 1996.