

Mobile IP and the IETF

Charles E. Perkins

charles.perkins@eng.sun.com

SUN Microsystems, Mountain View, CA, USA

I. Introduction

This is a report from your faithful IETF correspondent, covering some of the relevant events at the 42nd IETF conference in Chicago, IL. Milestones were reached, and promising new developments are taking shape. Chief among the milestones was the passage to Last Call of the mobility support protocol for IP version 6 (IPv6). New developments include accounting protocol extensions for Mobile IP, and interest forming around the possible convening of a BOF for IP and TCP over wireless links at the next IETF conference in December.

II. Mobile IPv6 goes to Last Call

Dave Johnson presented the recent protocol modifications for mobility support in IPv6, at both the Mobile IP working group and the IPng (IP New Generation) working group meetings. Recent modifications to the protocol include:

- Renumbering refinements, using the Binding Request message.
- Clarifications about interpretation of Routing Headers by the mobile node
- New definitions and extensions for Router Advertisements
- Definitions for anycast

II.A. Renumbering

Some refinements have been made for renumbering the mobile node's home networks. As before, the home agent is expected to tunnel a Router Advertisement to the mobile node. Now, in addition, the home agent includes a Binding Request in the tunnel header. This is followed naturally by the transmission of the Binding Update from the mobile node to the home agent, as the mobile node acts on the new information provided in the Router Advertisement. As always with use of the Binding Update, the mobile node asks the home agent to send a Binding Acknowledgement, so that both parties are assured that the renumbering has taken effect. Router Advertisements used in this way are *required* to contain security headers to insure that the mobile node can verify that the advertisement came from the home agent.

II.B. Neighbor Discovery

Certain changes have been made to the base Neighbor Discovery protocol. Since not all IPv6 routers are required to provide home agent services, an 'H' bit has been added to the Router Advertisement, which, when set, signifies that the router sending the advertisement is a home agent.

A small modification has been made to the Prefix Information Option packet format. Now, if the 'R' bit is set in the

header, the 128-bit prefix field contains a globally reachable IPv6 address of one of the router's network interfaces.

Typically, a router advertises itself periodically, at a rate possibly faster than indicated by the lifetime of the advertisement. It is important for a mobile node to know how long to wait for advertisements, since it might base decisions about its continued connectivity on the arrival of the periodic advertisements. In order to provide this information to mobile nodes, a router can include the Advertisement Interval Option in its Router Advertisements.

Lastly, a preference field was added to the Home Agent Information Option, which allows a home agent to specify how long it is willing to provide home agent services.

II.C. Anycast

As part of the Dynamic Home Agent Discovery mechanism, the home agents have been assigned a newly defined *anycast group*. Anycast, described in RFC 1546 [3], is an addressing mode by which a packet can be delivered to just one of the set of hosts that belong to the anycast group. This is in contrast to *multicast*, by which a packet is delivered to *every* member of the multicast group indicated by the multicast address.

A new IETF draft [2] reserves a range of *well-known* anycast addresses in every IPv6 subnet, in addition to the already reserved anycast address for all IPv6 routers on link. The newly reserved addresses are the greatest 128 addresses from among all those available within the range defined by the routing prefix for the subnet. The newly specified home agent address is number 126 in that range.

Neither working group raised any significant objections to these changes, nor had any other issues that needed resolution. It was agreed to put the proposals for Last Call in both working groups. If no problems arise, the protocols will have been sent to the Routing Area Director for presentation to the Internet Engineering Steering Group by the time this article goes to print. Free code is available from the CMU Monarch project at <http://www.monarch.cs.cmu.edu/>. Multiple independently developed and interoperable implementations are needed before the protocol can progress past Proposed status.

I think that, once the current protocol actions have stabilized, there are several future directions that have merit. First, the Home Address Option is likely to be inserted into every data packet in circumstances where it is used at all. Since it adds 18 bytes to every packet, this is a substantial penalty to pay. The penalty can possibly be circumvented by use of IPv6 header compression [1], but this has not been demonstrated nor analyzed to my knowledge. Furthermore, there does not seem to be much momentum gathering behind the deployment of IPv6 header compression; the penalty of using the Home Address option would only be avoided if most of the IPv6 hosts could do the decompression.

I have proposed (informally) a variation on the Home Address option which enables the correspondent node to acknowledge the receipt of the option, and furthermore to indi-

cate that it would maintain enough state to do the appropriate address translation at the IP level for subsequent packets arriving with the same source IP address (viz., the mobile node's care-of address). The lifetime assigned for such source address bindings would have to be carefully managed to avoid problems when the correspondent node is rebooted during UDP transactions with the mobile node.

III. AAA extensions for Mobile IP

Since the inception of the Mobile IP working group, there has never been very much emphasis on providing a usable accounting service for connectivity services provided to visiting mobile nodes. In fact, the foreign agent in Mobile IPv4 is modeled as a fairly neutral and passive device, not able to make any particular decisions on the acceptability of registrations attempted by the mobile node. More sophisticated interactions are not precluded by Mobile IP, and an authentication extension for use between the foreign agent and the mobile node was thought to provide enough of a hook for any further protocol development that might be needed for accounting purposes.

While this is true in an abstract sense, it does not take into account the rise of RADIUS and other dial-in accounting protocols for use with mobile laptop computers. Moreover, in today's market, many people equate dial-up computing with mobile computing; this has led to a situation wherein part of the mission of the Mobile IP working group has been taken up by participants of the *roamops* working group. Specifically, instead of using Mobile IP, a roaming laptop user is much more likely to dial up over a phone line, using PPP to establish the link. The NAS (Network Access Server) will then use an AAA protocol (e.g., RADIUS) to obtain assurance for payments, and to initiate accounting procedures relevant to the connection by the mobile node. Roaming users typically do not expect to maintain any previously established session, perhaps because such services have not been widely available. Furthermore, roaming users today are likely to need additional services not provided in Mobile IP, such as automatic allocation of a home address as part of the registration request process.

IV. Miscellaneous Mobile IP discussions

Two other presentations during the Mobile IP meeting were noteworthy. The first was Stuart Jacobs' proposal for using public key cryptography to enable the mobile node to authenticate itself to the foreign agent. This proceeds by involving a Certificate Authority (CA) (or, perhaps, more than one) in the registration process, that can vouch for the identity of the mobile node. There were major concerns about the performance and scalability of this approach. The hope is that new, fast processors can eliminate the concern about delays because of expensive exponentiation operations. The existence of a deployed hierarchy of CAs would make use of this proposal more realistic.

The other presentation was a novel method of introducing mobility into networks controlled by a Network Address

Translation (NAT) device. If all packets entering an administrative domain pass through the (same) NAT device, then the NAT device can be endowed with additional functionality to redirect traffic streams according to the current location of the mobile node. This design was chosen to support mobility without requiring modifications to the protocol stack of the mobile node. As with standard Mobile IP, the dangers of fraudulent *remote redirects* indicate a requirement for strong authentication in the (modified) Registration Request, which is then sent to a Registration Server (RS) on the home network. The RS then communicates care-of address information to the NAT device, and the NAT device subsequently translates the destination IP address on every packet bound to the mobile node, so that it becomes the care-of address instead. If the correspondent node has a private IP address, then packets delivered from a correspondent node inside the boundary defined by the NAT device require translation of the source IP address (the private IP address of the correspondent node) to another IP address (e.g., that of the NAT device itself), which is not a private IP address.

References

- [1] M. Degermark, B. Nordgren, and S. Pink. Header Compression for IPv6. draft-degermark-ipv6-hc-03.txt, July 1997. (work in progress).
- [2] D. Johnson and S. Deering. Reserved IPv6 Subnet Anycast Addresses. draft-ietfipngwg-resv-anycast-00.txt, Aug. 1998. (work in progress).
- [3] C. Partridge, T. Mendez, and W. Milliken. Host any-casting service. Request for Comments (Informational) 1546, Internet Engineering Task Force, Nov. 1993