

Mobile IP and the IETF

Charles E. Perkins

charles.perkins@eng.sun.com

SUN Microsystems, Mountain View, CA, USA

MILCOM '97

I was invited to participate at an ad-hoc network panel for MILCOM '97, held in Monterey. The military interest in ad hoc networking technology continues unabated. The panel was organized by Zygmunt Haas of Cornell University, who has also become active in the IETF manet working group. The panel included a wide diversity of viewpoints, but all panelists agreed that the general area is assuming greater importance as the military need for networking solution grows, and as the Internet becomes the communications technology of choice for data and soon multimedia transmissions. Contrasts were drawn between flat vs. hierarchical routing architectures, and on-demand vs. fully-maintained routing information. Hierarchical algorithms maintain node clustering information, which itself can be expensive to maintain if mobile nodes move between clusters very often. The advantage is that routes are then maintained only between cluster heads, so that routing tables are smaller and route updates have to be transmitted less often. The lack of quality of service (QoS) in existing protocols was lamented, and several suggestions were made that connections between the link layer and the routing protocols will be necessary to satisfy the physical realities of constructing ad hoc networks in the battlefield. Your mobile correspondent remains convinced that factors such as transmission power, asymmetric links, battery life, and quality of service cannot be integrated well into the routing protocols until we have a better understanding of the basic needs of highly dynamic routing. Once the easier cases are better understood, the additional complications can be studied much better.

The military panelists emphasized a wide range of specialized requirements that are unlikely to arise in commercial applications. For instance, there is a need for nodes to avoid detection, which translates into the need to use spread spectrum techniques at the link layer, and the need to minimize all transmissions at the network layer and above. Thus, traditional techniques for neighbor discovery (like periodic beeping) need to be re-examined. Furthermore, military ad hoc networks exhibit a wide disparity in the relative speeds of the varieties of mobile nodes, from jet planes to ships to armored vehicles to ground troops. To these problems, we must add the further requirements for secure communications, multicast, and the often expressed desire for multimedia communications. My sense is that the protocols under consideration in the IETF will not be able to meet all of the military's stated requirements for quite some time. On the other hand, military involvement in the IETF protocol standardization effort seems assured, and this panel discussion was among the most popular events at MILCOM this year.

Mobile IP working group

During the Mobile IP meeting, presentations were made about Mobile IPv6, route optimization, TEP (Tunnel Establishment Protocol), and two projects regarding security.

Dave Johnson (CMU) made the presentation about Mobile

IPv6. Mobile IPv6 was the most pressing agenda item, since it's our purpose to try to get the current draft into Proposed Standard status within the IETF. Recently modified areas of the Mobile IPv6 specification include the following:

- The new Mobile Home Address destination option allows mobile nodes to satisfy ingress filtering constraints. With this option mobiles can use their care-of-address in the source IP address of the IPv6 header instead of their home address, while still enabling correspondent nodes to maintain TCP connections via the mobile node's home address.
- The method of using a newly allocated anycast address for home agent discovery selected from among several competing alternatives (among which were encapsulating multicast within anycast, and new advertisement extensions).

Other discussion about when an IPv6 home agent should forward packets to the mobile node resulted in the conclusion that no link-local or site-local packets should be forwarded to the mobile node by the home agent UNLESS the home agent was (somehow) certain that the mobile node's care-of address was also within the same site as the site-local address of the mobile node. Interestingly, the Mobile Home Address option does not require authentication any more than vanilla packets sent to the correspondent node using the mobile node's home address as the source IP address. This results from the fact that the Mobile Home Address option has no effect on the handling of future packets (in contrast to the Binding Update option). Once the basic concept is accepted, I expect to propose a variation on the Mobile Home Address option that will affect future packet handling, which will then require authentication. The variation would allow the mobile node to have the desired effect on future packets to the correspondent node, without having to send the Mobile Home Address option each time.

Luis Sanchez (BBN) discussed a way to enable nodes other than the home agent to authenticate messages from the mobile node. The approach uses public key exchange to acquire tickets which are then used while the mobile node remains in the administrative domain for which the public key exchange is valid. This feature is indicated by new advertisements from the foreign agent. Your author believes there is a very close relationship between this work and the registration key Internet Draft described next for route optimization.

The IPv4 route optimization presentation detailed the split of the previous route optimization specification into three separate Internet Drafts. The first draft contains all the information about the transmission and use of Binding Updates, and the message used by foreign agents to effect smooth handoffs. The second specifies a number of ways to establish registration keys that can be used between foreign agents and mobile nodes to make the smooth handoffs secure. The third draft specifies "Special Tunnels", which can be used by foreign agents to avoid dropping packets destined for departed mobile nodes,

and which at the same time enable the home agent to avoid routing loops. Any protocol allowing routing loops is considered anathema within the IETF.

Pat Calhoun and I presented our Tunnel Establishment Protocol which we hope can extend the Mobile IP registration process to support multiprotocol mobility, regional registration, and remote/dial-up access to private networks. This protocol was also presented to the VPN BOF, further described later in this report.

John Zao (also BBN) presented their ideas about how to provide security for data tunneled between the home network and the mobile node. It was mainly presentation about integrating IPSec and Mobile IP tunnel management, with secure tunnel negotiations happening as part of the Mobile IP registration process.

Service Location working group

The Service Location working group continues to attract growing interest. Topics considered include IPv6, Wide-Area service location, the API document, trust models and digital signature operations, a new scope model, and the creation of SLP version 2. Several pressing protocol problems have prompted the creation of SLPv2, and since the meeting in December the new draft has been motivated, discussed, created, revised, and published. One of the important features of the SLPv2 is that the broken character-set support devised for SLPv1 (RFC 2165) has been eliminated. Now there is just UTF-8 (containing US ASCII as a subset). The IPv6 draft has gone to Last Call – but there's not much going on in IPv6 that is any different from SLP for IPv4, since use of IP addresses does not play a prominent role in the protocol.

One of the main point of discussion revolved around a newly proposed model for “scopes”, which are basically sets of services useful for administering the network. Acting upon a suggestion by Tom Narten (one of our benevolent Internet Area Directors (AD)), the authors of SLPv2 revamped the scope model so that now (essentially) every service is presumed to belong to a scope. If no scope is explicitly assigned, the service belongs to a “default” scope. This is different than in SLPv1 for two reasons:

- In SLPv1, it was possible for services to have “no scope”, which meant that they would respond to Service Requests regardless of what scope was specified, and
- In SLPv2, a service does not respond to Service Requests unless the request was made for service from a matching scope.

The latter works O.K., because unless scopes are explicitly configured, all User Agents, Service Agents, and Directory Agents use the default scope.

TEP/VPN BOF

Since tunneling is important for mobility, and for remote access to enterprise networks, it is natural that Mobile IP's registration procedure also be considered as a tunnel establishment protocol (TEP) for remote access. Furthermore, there is a close relationship between the problems of remote access, and creating virtual private networks (VPNs) by tunneling between topologically separate routing domains. Since we have

created TEP to begin to address the needs of mobile nodes and remote access, I presented the basic protocol design at the recent IETF BOF on VPNs. What I expected to be a popular but specialized gathering for the purposes of discussing tunnels, turned into one of the major events of the IETF meeting. The originally scheduled room was no match for the 1000+ people who showed up for the discussion, a circumstance that your author found slightly intimidating as a forum for presentation of our less than fully-baked results.

A list of VPN issues discussed at the BOF should look quite familiar to mobile networking researchers:

- Tunnel Establishment
- Network Address Translation (NAT)
- Securing the traffic (or, how to actually use IPSec)
- Quality of Service
- Naming (especially the desired tunnel endpoint)

No one seems to have a very good idea about whether all of these issues are able to be accomplished in the near or medium term. Mobile IP, in my opinion, needs to pay careful attention to the outcomes of any future VPN working group, since mobile nodes are likely to be connected into enterprise networks by way of VPNs. The new working group will also pay attention to various tunneling protocols like PPTP and L2TP, and these alternative tunneling protocols should also be scrutinized for possible use within the framework of Mobile IP. Tunnel establishment, configuration, management, and shutdown can all be fruitfully modeled as operations controlled by extensions to Mobile IP's Registration Request message, and that is the philosophy espoused by TEP (along with some ways to reduce registration traffic to and from the Home Agent).

The issues surrounding NAT are also issues that face Mobile IP. Just as one simple point of interaction, what happens if a foreign agent tries to offer service to two mobile nodes that just coincidentally have the same IP address drawn from different administrative domains? The IP addresses of the mobile nodes are unique enough within their home domain, but not once the mobile node roams away from home. Some people say that's a good reason to avoid NAT. I say it's a good reason to modify Mobile IP.

Announcements

• “Mobile IP: Design Principles and Practices”

I finally finished the book I'd been working on for so long. It's published by Addison Wesley. You can find more information by following the link from my web page, indicated below.

• Workshop on Service Discovery in the Internet

I'm organizing a half-day workshop on the subject of Service Discovery, to be held in conjunction with the 4th annual MobiCom conference this year in Dallas (Oct. 25 - 30). Anyone who is interested in participating please let me know. Details will be posted to the MobiCom '98 Web page:

<http://www.mobicom98.utdallas.edu/workshop.html>,

and are accessible now from my web page:

<http://www.svrloc.org/charliep/workshop98>.