Secure Mobile Networking 9th Quarterly Report*

James R. Binkley and John McHugh
Portland State University

4 February 1998

Project Status Overview

We operated during this quarter under the assumption that there might be no additional funds forthcoming for FY 98. Under this assumption, we would have had barely enough funding to continue support of our existing students through their scheduled graduation dates. In early January, we received an additional $75,000 (including overheads) which will allow completion of work currently under way and at least two additional releases of our system. It will also allow modest improvements in our equipment base.

In summary, we have slowed down quite a bit due to the programmers departing at the beginning of the quarter. We have three M.S. graduate students working on certain aspects of the mobile project at this point. Two of them will graduate at the end of the winter quarter and one will remain until the end of the spring quarter. It should be pointed out again that we made a combined release of Mobile-IP/IPSEC last summer and those files remain available at PSU and MIT.

Bill Trost and David Reeder left us at the beginning of the quarter, which was probably a good thing as we had no money to pay them. David Reeder is now employed at Trusted Information Systems. Jim Binkley is working as a combination faculty/network engineer job at Oregon Graduate Institute, and it still helping to author academic papers with John McHugh and Sarah Mocas and oversee our remaining project graduate students at PSU. The graduate students are Jennifer Ye, Zheng Chen, and Bjorn Chambless.

We have wrapped up work for now on our Multicast Ad Hoc Routing Protocol (MADRP) (Jennifer Ye is the graduate student). Jennifer tied the multi-hop ad hoc routing protocol to Mobile-IP and to IPSEC tunnels. A remote mobile node that is greater than one hop away from other mobile-node can setup 2-way ESP tunnels to other mobile nodes. It can also connect to the Internet via a Mobile-IP agent that is not directly hearable. This work is checked in and will be made available in a next release. At some point, we would like to write a paper on this effort, but are unsure as to when we might have time.

Bjorn Chambless has just about completed his work on the Home Agent Redundancy Protocol. The code has been checked into the source base. Bjorn still needs to successfully

*Supported by th U.S. Department of Defense Advanced Research Projects Agency and the U.S. Air Force Rome Laboratory under contract F30602-95-1-0046.

deploy the HARP protocol internal to both PSU and OGI mobile-IP systems; i.e., have two cooperating HAs in both cases. He also needs to demonstrate that a routing daemon (say routed running RIPv2) can co-exist with the PSU mobile-ip agent routing daemon (mipd). Bjorn and Jim Binkley co-authored a draft RFC that describes HARP (draft-chambless-mobileip-harp-00.txt). The document has been submitted to the IETF.

Zheng Chen has finished work on a simple authentication protocol for Mobile-IP that uses DNSSEC based public-key cryptography. The work is not checked in as of yet and it is not clear to us exactly how we might distribute it. He has helped to author a paper on the subject of public-key crypto and Mobile-IP with Sarah Mocas which was submitted to the Oakland IEEE Security conference.

Zeng Chen has begun work on supporting DHCP (Dynamic Host Configuration Protocol) in Mobile IP. Mobile Hosts use the protocol to obtain temporary addresses at foreign networks for routing purposes but still maintain "permanent" home addresses for identity purposes and keep continuous transport layer connectivity while moving. This way, the Mobile Node can acquired a "co-located-care-of-address" at the foreign network and can detunnel packets itself. This work will continue during the Winter quarter as noted below.

Next quarter plan

Bjorn will finish working on HARP and get it deployed with Jim's help so that we have dual HA's at PSU and OGI. It is important here to demonstrate that the HA can actually participate in an interior routing domain protocol and the implementation side of that statement is not straightforward. With the cooperation of network engineers in the engineering school at PSU, we will attempt to teach the local ciscos to accept route changes forwarded with RIPv2 from the FreeBSD based mobile routers. Thus HARP can interact (courtesy of the FreeBSD routed) with the interior gateway routing scheme in engineering. We are choosing RIPv2 for this experiment, because we must use class C based subnet masks, and because we might have to modify routed to teach it to ignore Mobile-IP tunnel routes.

Bjorn will be with us for two more terms. As a consequence, we have appointed him wireless system administrator with the task of keeping the wireless network system up including laptops and agents. He is also going to attempt a minor port of the mobile node daemon (the laptop Mobile-IP daemon) to linux. If he can do this, researchers at OGI (who use linux) will consider running our version of Mobile-IP.

Zheng Chen is going to use his remaining quarter to investigate the routing issues of combining DHCP support with our Mobile-IP routing setup (at laptops). He will also briefly investigate security considerations in this regard. We regard this as major redundancy work as the resulting laptop system should be able to work on either a Mobile-IP agent/beacon link or a DHCP (local IP address) link and dynamically switch between them when roaming. Our resulting Mobile Node daemon will have a simple DHCP client capability that will enable it to dynamically attempt DHCP hookup when Mobile-IP agent advertisements are not heard. We would then expect to tunnel back to our Home Agent as a very simple way to keep connections using the Mobile-IP "home" address alive.

Effectively such a mobile system becomes at least multi-homed; i.e., it will have a local and short-lived IP address used to talk to local systems and a global and long-lived IP address that is its Mobile-IP address. How to deal with such a situation is not clear in a routing sense (Please see the excellent "Internet Mobility 4x4" paper by Stuart Cheshire and Mary Baker under `http://rescomp.stanford.edu/ cheshire`) as fundamentally a policy mechanism that will allow transport-side applications (TCP/UDP) to choose a long-term or short-term IP address must exist. Further, security considerations are challenging in terms of possible policy. One simple mechanism might be to simply use the local IP (DHCP-gained) address to tunnel all "real" packets home so that they will appear on the Internet with the permanent home address. We will explore this latter option.

Jennifer Ye has started working on Foreign Agent redundancy. What we mean by this is the fundamental ability of a Mobile Node to use at least two agents as link attachments; .e.g., a wireless node might keep the best two agents in terms of signal strength and send packets to both of them. This work must be done in two stages:

1. A kernel routing mechanism must be created that allows a BSD route to have two gateways so that when IP encounters such a route, it will duplicate the packet and send it out the interface pointed to be the second gateway. Note that this gives us the extremely interesting capability to actually use two interfaces at once with possibly different links. This capability is not very different from the situation where a high-level routing protocol like OSPF must do packet load sharing to a remote but equal cost destination. Of course, in our case every outward bound packet will be duplicated. This is very selfish from the Mobile Node's point of view. We are effectively prioritizing its individual communication over the entire internal network bandwidth. Still, such a capability could be useful where links are stressed and command communication is important.

2. Mobile-IP must take advantage of this kernel capability. For example, we would take advantage of our existing ability to prioritize agents by signal strength and instead of using the best, use the top two. Home Agents must also support dual Mobile-IP registration.

If there is remaining money for one more graduate student, we might hire such a person to keep the project going. That person could conceivably take over Jennifer's work in the Foreign Agent redundancy area.

John McHugh, Sarah Mocas, and Jim Binkley are writing a high-level paper on mobile security policy. We will attempt to get this paper finished this quarter and submitted to a an appropriate journal. If time permits, the HARP draft will be converted into a paper and submitted to a wireless journal as well. Jim and David Reeder are going to attempt to collaborate with John Zao of BBN on a IETF draft that addresses certain Mobile-IP and IPSEC combinatory issues.

At the end of the winter quarter, we will bundle up another release of our software and make it. Minimally that software will include HARP and MADRP and may include other features if complete and in time.

Outreach

We have been contacted by a number of groups or people regarding our current efforts including Berkeley/South Carolina University/BBN and elsewhere and have attempted to provide information as possible within our time limitations. Lixia Zhang's research group at UCLA has made use of our tunnel driver code in FreeBSD. The latest release of FreeBSD contains the ISA wavelan driver that Jim Binkley ported to FreeBSD long ago.

We are attempting to locate an industrial partner in the cellular telephone field to partner on a proposal to PATH, the automated highway research group at Berkeley. The proposal would be to investigate extending Mobile-IP to provide cost effective internet access to mobile units on the highway. A key feature would be extension of FA beaconing to provide for local emergency and commercial notifications.

Jim Binkley and Bjorn Chamblis have written an internet draft on HARP which appears as an appendix to this report.

Equipment

Our equipment, especially laptops, is suffering from near obsolesence. Many of the laptops are over two years of age at this point and we note that the average laptop lifespan at this point seems to be (less than) a year. Our wireless network situation is made more complex by rumors that Lucent may stop selling the 915mhz equipment in order to centralize on IEEE 802.11 and 2.4 ghz equipment. This would effectively give us no way to keep our network up for research without replacing it. We hope that we might obtain a small amount of money to buy a few laptops, cheap desktops for agents, and some replacement 915mhz equipment.

The HARP Draft

Internet Engineering Task Force   Bjorn Chambless
INTERNET DRAFT   Portland State University
Jim Binkley
Oregon Graduate Institute
October 27, 1997

HARP - "Home Agent Redundancy Protocol"
<draft-chambless-mobileip-harp-00.txt>

Status of This Memo

Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet Drafts are draft documents valid for a maximum of six months, and may be updated, replaced, or made obsolete by other documents at any time. It is not appropriate to use Internet Drafts as reference material, or to cite them other than as a ''working draft'' or ''work in progress.''

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

This document presents a protocol called the Home Agent Redundancy Protocol or HARP. HARP is an optional extension to Mobile-IP [RFC-2002]. Mobile-IP includes the notion of a Home Agent which is a host located on the home IP subnet for Mobile Nodes. Home Agents forward packets to Mobile Nodes that are away from home. Since Mobile Nodes are dependent on the Home Agent for connectivity when away from home, the Home Agent represents a possible single source of failure for the Mobile IP system.

HARP is a protocol which allows a pair (or set) of Home Agents to cooperate and share Mobile-IP Mobile Node registration information. If one of the HARP peers should fail, the Mobile-IP

system will not necessarily fail, hence HARP introduces Home Agent redundancy into the Mobile-IP system. Mobile Nodes are not aware that HARP exists, so HARP requires no changes to Mobile-IP as a protocol. In this document, we present the HARP architecture and protocol.

Table of Contents

1. Introduction

Mobile-IP is designed to allow a Mobile Node (MN) to change its point of IP subnet attachment in the Internet at the network or IP layer. The MN is always identified by it home IP address regardless of its current network location. Its mobility is not limited by conventional IP network boundaries.

The Mobile-IP system consists of Mobile Nodes, and two kinds of agents, known as Home Agents (HA), and Foreign Agents (FA). Home Agents remain "home" and when the Mobile Node is not home, forward packets sent to the conventional IP subnet of the Mobile Node to a possibly distant point of attachment. The remote address is called a Care Of Address (COA), and may be at a Foreign Agent or a co-located Mobile Node. As a Mobile Node travels from one IP link to another, it determines possible COAs and uses the Mobile-IP registration protocol to inform the Home Agent of its current location. The Home Agent then forwards packets addressed to the Mobile Node at its home network to the its current location.

In Mobile-IP, as currently specified, a single HA services an MN. The MN is reliant on this Home Agent for its connectivity. Thus the HA represents the possibility of a single point of failure for Mobile-IP. A Home Agent may be responsible for multiple Mobile Nodes on multiple home subnets. The failure of a single HA may then result in the loss of connectivity for numerous Mobile-IP Mobile Nodes located throughout the Internet. Thus the Home Agent and Mobile Node taken together have a shared fate. A Mobile Node cannot afford the loss of its Home Agent.

This vulnerability is inconsistent with the fault tolerant nature of the Internet. Additionally redundancy is needed. We have developed the Home Agent Redundancy Protocol (HARP) as an optional extension to Mobile-IP to address this problem.

HARP is a simple protocol based on the notion of one or more HARP peers that act as a single shared Home Agent. Each HARP peer is configured with information about its HARP peers and forwards any Mobile-IP registration messages it receives to its peers. HARP peers act in parallel to create or delete tunnels [RFC 2003] to the Mobile Node's remote COA according to the last registration message received. Although we speak of HARP peers as a set, in general, there will probably be only two cooperating systems in the HARP sub-system.

There are three major types of messages, 1. HARP TCP DUMP, 2. HARP UDP FORWARD., and 3. HARP UDP PING. At boot, a TCP connection may optionally be made to a remote HARP peer to exchange mobile routing information. At runtime, HARP UDP PING messages are exchanged to determine if remote HARP peers are up. At runtime, HARP UDP FORWARD messages are used to forward Mobile-IP registration messages from the receiving HARP agent to its HARP peers.

HARP assumes no changes to Mobile-IP proper; i.e., the existence of one or more HARP peers is kept hidden from Mobile Nodes. Therefore HARP will interoperate with existing Mobile-IP implementations. In routing terms, one may think of the HARP peers as advertising the existence of a common IP subnet into an interior routing domain. Externally, a MN's Mobile-IP authentication message is routed to the nearest (according to local routing metrics) HARP peer which, in turn, informs other HARP peers about the MN's location via a HARP FORWARD message. Packets are routed to HARP peer Home Agents via conventional routing, and since each HARP peer maintains Mobile Node COA information, packets are forwarded to the MN.

1.1 Design Goals

The Home Agent Redundancy Protocol (HARP) aims to remove the Home Agent as a single point of failure for Mobile-IP.

The protocol is implemented entirely through the enhancement of Home Agent functionality. There are no additional responsibilities or modifications required of either Mobile Nodes or Foreign Agents. Mobile Nodes and Foreign Agents have no knowledge of HARP and Mobile-IP will interoperate with HARP capable Home Agents.

The Home Agent Redundancy Protocol will be made secure, minimally with authentication, and optionally with authentication and privacy mechanisms.

Home Agent Redundancy makes no assumptions about the physical media utilized by the Mobile-IP environment. Therefore HARP does not limit the physical implementation of Mobile-IP.

The number of Mobile Nodes is not limited by HARP.

1.2 Terminology

Home Agent Redundancy Protocol terminology uses and expands on the Mobile-IP terminology presented in RFC 2002. The following terms are specific to the Home Agent Redundancy protocol:

HARP peers -
co-HAs -
co-Home Agents - A set of Home Agents acting in concert

to provide connectivity to one or more Mobile Nodes. These hosts share an IP address on the Home Subnet but each has a uniquely identified interface outside of the Home Network. Co-HAs, a priori, know about a small set of cooperating Home Agents and exchange registration information regarding Mobile Nodes and periodically test peer co-HA reachability. One may assume that there are only two Home Agents in a set of co-HAs, but there is no inherent limit to the number of peers in a Co-HA set.

Primary-HA, Primary - The Home Agent of a co-HA set which is currently receiving registration information directly from a MN. The Primary Home Agent shares this information with its co-HAs (Secondaries) by forwarding registration packets to the peers. A HA is primary because the IP routing infrastructure is currently routing the Mobile-IP registration packet to it.

Secondary-HA, Secondary - A Home Agent of a HARP set which is receiving registration information about a given MN indirectly through its co-Home Agent which is acting as the Primary.

HARP - Home Agent Redundancy Protocol.

HARP PORT - The HARP port number which is the same for both the TCP and UDP ports. This port has not yet been allocated yet.

Home Network - Home Subnet - The subnet containing both Home Agents and the home addresses of the Mobile Nodes they are serving. This subnet may be partitioned in terms of the co-HAs or the co-HAs may be physically present on the same link.

Partitioned Subnet - A physically divided Home Subnet. Home Agents in a co-HA pair may be thought of as existing on a virtual subnet. Physically divided means that the co-HAs cannot use that link to communicate directly. Note that this is not a requirement of HARP, but an aspect of network design. We will discuss the network design aspects of HARP below.

AWAY(Mobile-IP state) - The state of a Mobile Node, with respect to its Home Agent(s), in which datagrams addressed to the MN arrive at its Home-Subnet and are tunneled to the MN's Care Of Address by one of the Mobile Node's Home Agents.

AT HOME (Mobile-IP state) - The state of a Mobile Node with respect to a Home Agent in which the MN's current point of attachment in the Internet is consistent with its IP address. In this state, the Mobile Node will receive packets directly.

At CoHA(Mobile-IP state) - The state of of Mobile Node, with respect to a Home Agent, in which the MN's home subnet is partitioned and a packet arrives for the MN at another link of the partitioned network. In this case, packets addressed to the home subnet may arrive on a portion of the home subnet to which the Mobile Node has no link layer attachment. These packets must then be forwarded (tunneled) by one HARP peer to another.

2. Protocol Overview

This section provides a protocol overview of HARP. We discuss HARP from a routing topological point of view, and provide a short discussion of redundancy issues.

2.1 Assumptions

The following are fundamental assumptions about the design of a HARP redundant agent network:

1. So that Mobile-IP and Mobile Nodes need not know about the HARP sub-system, we assume that the HARP peers share a single IP subnet and a single IP network address.

2. Due to assumption 1, and because the HARP agents must communicate amongst themselves, we assume they are multi-homed in the sense that there exist on one node at least two IP addresses. We will call them the "Mobile-IP subnet" address, and the "HARP peer" address. The former is shared. The latter is not shared. The HARP peer address is unique and is used by HARP systems to communicate amongst themselves. Note that this does not rule out an agent with only one physical interface.

3. We assume that the HARP peers exist within an interior routing domain that runs a IP interior routing protocol such as RIPv2 [RFC-1721], or OSPF [RFC-2178]. Thus packets addressed to the Mobile-IP subnet, including Mobile-IP authentication packets, are routed to the HARP peers according to the local metrics of the interior routing protocols. At any given time, any packet bound for a Mobile Host at HOME, will go to exactly one HARP peer. Ideally, if an interior link fails, an interior routing protocol will switch Mobile-IP packets to the other HARP system. This does not rule out the possibility of HARP being used with static routes in interior routers. External routes to the Mobile-IP subnet may always be changed by hand in the event of HARP agent failure.

Finally, it is NOT assumed that the HARP Mobile-IP subnet is partitioned. Partitioning may add useful redundancy attributes. But the subnet need not be partitioned. How this is handled is implementation and site specific and will be discussed more in the next section.

2.2 Protocol Overview

Diagram 1:

```
                         MN or CH

                            |
                            |  MN/CH path
                            |

Internet

                            |
                            |
                            |
                 ------------------------
                R1    interior path      R2
                |                         |
 H1                      H2
                |                         |
               ----- Mobile-IP subnet ------
```

Please refer to diagram 1 for the following discussion.

Assume we have a Mobile Node that is away from home. Assume that at home we have two routers R1, and R2, which are using a local interior routing protocol (for example, OSPF, or static routes). Behind them are two HARP peers which advertise a Mobile-IP subnet to the routers and to the network. Along with the Mobile Node on the exterior Internet, there exists a Correspondent Host (CH). The latter is any host interested in sending packets to the Mobile Node.

The Mobile Node is unaware of Home Agent redundancy and sends registration information only once to the shared HA address located on the Home Subnet. Due to the nature of unicast routing, this information may be received by either Home Agent, but is likely to be received by only one. Packets sent from the CH to the Mobile Node will likewise be routed to one or the other Home Agent (whichever is "closer", according to the metrics of the interior routing system). Note that any of these datagrams (Mobile-IP authentication or ordinary datagrams) may at any time go to either Home Agent.

When a Mobile-IP registration packet is received by a co-HA, it will encapsulate that registration packet and forward it to another co-HA via the HARP UDP port. Thus the peer co-HA will know that the other HA directly received the registration, and will also know the current MN Care Of Address; i.e., the forwarding address for CH packets.

Each HARP peer takes the same internal action whether it receives a Mobile-IP registration packet directly from a MN or whether it receives it from a HARP peer. For example, in parallel, the Mobile-IP vlist entry is created or refreshed, and tunnels are setup (if needed) from the Home Agent to the Care Of Address. In Mobile-IP terms, the Home Agents act in parallel.

Mobile-IP authentication (MN to HA, FA to HA, etc.) is performed once at the primary co-HA system. The secondary is expected to perform a separate HARP protocol authentication (HA to HA) on packets forwarded to it by the primary via the HARP UDP (or TCP in the case of table exchanges) ports.

If one Home Agent should fail, the interior routing structure should notice that it has failed as a router, and normal routing convergence will remove that path to the Mobile-IP subnet.

Convergence may take manual route manipulation in some cases where static routes are used. As a result, the Mobile-IP system should be able to survive the loss of a Home Agent as packets will be routed to a surviving Home Agent.

HARP consists of three major packets type sent from one HARP peer to other HARP peers. (Note that some of the types have acknowledgements). We have already mentioned the HARP UDP FORWARD, which is a simple repackaging of the Mobile-IP registration packet itself. In addition there are two other kinds of messages used in the HARP system. There is a HARP PING and a HARP boottime table exchange. The former uses UDP and the later uses TCP.

The UDP HARP PING is used to determine if other HARP peers are up. If a PING fails (say 3 out of 5), a HARP agent knows that either its peer has failed or the path to it has been partitioned. It may then take implementation-specific actions which should include ways to attempt to notify local administrators that critical interior links or systems have failed. Other implementation actions may be taken as well if needed. For example, a dormant local link interface might be enabled.

HARP provides an optional boot protocol which uses TCP to exchange all HARP information in one connection. Thus if one HARP system reboots after failure, it can acquire Mobile-IP state information from another HARP peer. At boot, a HARP Home Agent will attempt to establish a TCP connections with its co-HAs at their respective TCP HARP PORTs. If successful, these connections are used to pass all current Mobile Node registration information from a running HA to a booting co-HA. When all relevant information has been passed, and the booting Home Agent is synchronized with respect to MN Registrations, the TCP connections are closed. If the peer system is not available, the sending system will timeout and proceed as the peer may be unavailable or rebooting.

2.3 Redundancy Considerations

There are a number of redundancy considerations regarding HARP that have driven its design which we will present in this section.

The failure of one HARP agent, or a network interface on that agent, or possibly a path to that agent should not necessarily cause the Mobile-IP network to fail. This is, of course, the goal of the protocol itself. In addition to simple node redundancy, redundancy may be possible if a path from the MN (CH) in question exists to another HARP agent even when an interior (or exterior) router (or associated interface) fails. Thus HARP may sometimes be able to take advantage of dynamic interior routing.

On the other hand, the interior path between the HARP agents should not be allowed to fail. If it does, it is possible that the Mobile-IP registration packets might go one way and datagram packets from a given CH might go another, thus leading to a (bizarre) partition. This is one of the reasons for the HARP PING protocol. Lack of connectivity between the agents should lead to a local management alert. Of course, fundamentally, an interior path failure might cut the Mobile Node off from important local services and should be taken seriously in any case.

As part of the overview, we should justify why we have chosen UDP for internal HARP forwarding as opposed to say TCP connections between HARP agents. We felt that the HARP protocol should internally match the design of Mobile-IP. Registration for Mobile Nodes while away from home is driven by Mobile-IP/UDP based packets. Since the Mobile Node drives the registration, we felt that forwarding these packets internally over presumably shorter channels (with higher bandwidth) was reasonable. As a result, Mobile-IP registration also drives the HARP sub-system. We also felt that given the goal of producing a reliable server with reliable software it made more sense to use a simple protocol without the enhanced complexity of a TCP state machine to deal with possible protocol errors. Thus agent-side implementation should be simpler. As a final point, even though the number of HARP peers in a HARP set is likely to be very small, at some future time, one might consider experimentally replacing the unicast UDP HARP (re)registration with reliable multicast registration. Of course, TCP lacks multicast capability.

Redundancy considerations for the Mobile-IP home link itself are discussed in the next section.

3. Mobile-IP Home Link Considerations

One might claim that the impact of HARP on the actual Mobile-IP home subnet link could be regarded as implementation dependent. This is because Mobile-IP itself is aimed not so much at dealing with how mobile nodes interact at the home subnet, but how they can take a home subnet IP address, move to other subnets, and retain connectivity. Thus HARP primarily seeks to address the problem of what might happen if the home forwarding agent is lost. Still, the issue of redundancy on the Mobile-IP home link exists and there is a small amount of protocol impact on HARP. In a very simple sense, having two possible "home" links can aid redundancy as well. If one home fails, a second home might be available. In this section, we will discuss this issue and make implementation suggestions.

In the end local network management must decide what they want, according to available local resources and local tradeoffs. Therefore we suggest that implementations remain flexible where home subnet design is concerned.

The Home Mobile-IP subnet may be either:

1. not partitioned; i.e., the HARP Home Agents could reside on the same link and would be able to reach each other on that link.

2. partitioned; i.e., the HARP Agents might reside on different links, and would NOT be able to reach each other on that link.

3.1 Non-Partitioned Home Subnet

If the link is not-partitioned, the HARP Home Agents can reach each other directly. It is not advisable to have both HARP IP interfaces (which by definition share the same IP interface) active as confusion with nodes on the shared subnet might result. If the systems act as routers only (and not as end systems), one might claim that it would not matter, but there is no point in having both systems race to answer ARP [RFC-826] requests. Worse, any node that attempted to directly connect to the shared HARP subnet IP address with a transport protocol may experience failure due to ARP cache overwrites.

Thus it is reasonable to assume an implementation might provide a way to shut down one HARP interior IP interface and dynamically bring another up if failure of the other HARP node is detected. This can be done by the normal method of designated router election. A set of HARP peers exchanging HARP PING messages may choose the HARP peer with the highest IP address to be the only active peer on the interface. We assume that the PINGS are done over the non-Mobile-IP (and non-shared) IP address. If PINGS fail from that interface, (say after N failures, where N is configured in), the remaining HARP peers would again elect a designated router which will take over the "live" ARP function.

3.2 Partitioned Home Subnet

If HARP peers exist on the same link, it is possible that the failure of an interior router or router interface could lead to the loss of all HARP agents. Thus one may have replaced the Mobile-IP single point of failure mode with a more elaborate single failure mode. We suggest that if practicable (and this ultimately depends on per site network resources), it may be better to partition the home mobile link. In other words, the internal path to the HARP agents would still be an interior routing path, but the agents themselves might best be in widely dispersed locations. For example, HARP peers would be placed behind different interior routers, possibly in different buildings.

Such a partitioned network is not ideal for non-Mobile nodes, as IP subnet reachability problems would result if non-Mobile nodes were placed on the Mobile subnet. As a result, one might choose to only place Mobile-IP nodes on such partitioned links.

Where a partitioned scheme is used, it is necessary for the Home Agents to install tunnels between themselves. This mechanism is directly analogous to the Mobile-IP tunnel from the Home Agent to the Foreign Agent. A packet sent to a co-HA where the MN is not resident, would be forwarded to the other co-HA. Note that HA tunneling is not strictly necessary when the Mobile subnet is not partitioned, unless the Home Agents are only speaking one at a time to the home link.

A simple and less elegant solution would be to disable Mobile-IP router advertisements for Home Agents where actual physical residence is not desired. A dynamic scheme for election here could be used, or this function could be done manually. For example, one might choose to have only one Mobile-IP home subnet from the interior point of view. The other home might reside on a virtual interface that is not directly accessible except in the exterior routing sense. Mobile Nodes in such a system might never be able to directly visit the second home.

In summary, where interior router resources exist, partitioning may provide greater surviveablity.

4.1 Message Types and Functions

The Home Agent Redundancy Protocol has five messages:

HARP_FORWARD - This message consists of an encapsulated Mobile Node registration message which is tunneled from the receiving Home Agent to its co-HA. This information is used to update the co-HA's registration tables. This message type uses UDP and is sent to the HARP UDP PORT.

HARP_PING - This message is sent at configurable intervals from one co-HA to another to confirm connectivity. If the Home Agent receives no response from its co-HA peer, the co-HA is assumed to be unreachable. This message type uses UDP and is sent to the HARP UDP PORT.

HARP_ACK - Sent in response to a HARP_PING to acknowledge that the PING message has been received. This message type uses UDP and is sent to the HARP UDP PORT.

HARP_REG_REQ - A message requesting all Mobile Node registration information. This is the first message sent upon establishment of an inter-co-HA TCP connection. This message type utilizes TCP.

HARP_REG_DUMP - TCP message which contains Mobile Node registration information maintained by a Home Agent. This message is sent in response to a HARP_REG_REQ. Note that more than one DUMP message may be sent, but each DUMP message may contain more than one Mobile-IP node registration.

4.2. Message Formats

All HARP messages are structured in a Tag, Length, Value format.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type      |    Length     |    Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type and Length occupy one unsigned short and are 16-bit values. They are assumed to be in network byte order. Messages are sent to either the HARP UDP or TCP PORT.

4.2.1. HARP Registration Forward (HARP_FORWARD)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type=HARP_FORWARD         |     size                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Mobile-IP registration packet ...              |
|                                                               |
```

type: HARP_FORWARD = 1
size: in bytes of the value field.
value: Mobile-IP registration packet.

HARP Registration Forward messages are used to encapsulate and forward registration updates received from a Mobile Node. They are sent between co-HAs. The message consists of two bytes of type followed by two bytes indicating the length in bytes of a Mobile-IP registration packet. The Data field is a Mobile-IP registration packet of the size indicated by the size field. The registration packet has the same format as used with Mobile-IP. Optional (TLV) elements may be present and should be processed. However it is expected that the receiving Home Agent deals with all MN/HA and MN/FA authentication and may remove those elements from the registration packet.

4.2.2 HARP Ping (HARP_PING)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type=HARP_PING            |       size=4                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     HARP peer IP address           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

type: HARP_PING = 2
size: 4
value: (reachable) IP address of HARP sender

HARP_PING messages are sent between all the members of a HARP co-HA set. They are sent with a configured periodicity and are sent within a configured mechanism for determining the loss of an interior routing path. For example, one might send one message a minute, and retry N times. If the sending agent determines that another agent is down, it may initiate implementation-dependent mechanisms including SNMP alerts, paging a network administrator, and/or taking up or down a local interface. We include the HARP peer IP address in order to limit possible problems caused by multi-homing.

4.2.3. HARP Ping Acknowledge (HARP_ACK)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type=HARP_ACK             |        size=4                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     HARP peer IP address           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

type: HARP_ACK = 3
size: 4
value: HARP peer IP address

A HARP Ping Acknowledge message is sent in response to a HARP Ping. The peer IP address belongs to the sender of the acknowledgement.

4.2.4 HARP Dump Request (HARP_DUMP_REQ)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type=HARP_DUMP_REQ     |        size=0                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

type: HARP_DUMP_REQ = 4
size: 0

The HARP Dump Request message consists of two bytes of type followed by two bytes giving the size of the data field, which is always zero.

A HARP_DUMP_REQ is passed from a Home Agent in Initializing State to its co-HA through the inter-co-HA TCP connection. If the receiving co-HA does not receive this message, it should shut down the connection and log an error. If the client's connection fails or no DUMP appears within a configured timeout interval, the client should disconnect and log an error.

4.2.5 HARP Registration Dump (HARP_REG_DUMP)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type=HARP_REG_DUMP      |         size=8                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Number of Registrations                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Size of Registrations                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Mobile-IP registration field ...            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Mobile-IP registration field ...            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       etc.                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

type: HARP_REG_DUMP = 5
size: 8
value:
   Number of Registrations: a 32-bit unsigned integer in network
      byte order
   Size of Registrations: a 32-bit unsigned integer in
network byte order. This field contains the size of all
      the Mobile-IP registration sections which must all have
      the same size.
   Some number of Mobile-IP registration requests.

A HARP Registration Dump message is sent in response to a TCP connect and HARP Dump Request. It contains current registration information for all Mobile Nodes serviced by a given Home Agent. "The number of registrations" field tells the receiver how many registration messages are being sent. The size of the registration message gives the size of each Mobile-IP registration message which as before, is assumed to be the same format as is used with Mobile-IP. Note we assume that all message sub-fields are of the same length. Also note that a Home Agent need not write all of the information with the same TCP write. Nor does the responding peer need to send all Mobile-IP registration messages in one DUMP message. Multiple DUMP messages may be sent over the same connection.

The channel must be closed by the receiver when it has written all of the messages.

5. Security Considerations

In this section, we briefly consider the security of the HARP protocol itself. Security might also be taken to mean "survivability" and we will discuss that notion first, and then return to HARP protocol network security.

In terms of survivability, HARP primarily addresses the problem that a Mobile-IP system, serving a given number of Mobile Nodes may fail due to the loss of a single Home Agent. Home Agent redundancy reduces the odds of a total Mobile-IP system outage due to failure of a Home Agent node, a network adapter on that node, or possibly an internal routing path to that node. Given that we may have multiple Home Agents that cooperate to emulate a single home agent there may also be additional security benefits. For example, a denial of service attack against one Home Agent may not apply to the other (perhaps if they are not on the same link). Hence the Mobile-IP network might continue to function.

For protocol security of HARP itself, we require the use of IP layer security [RFC 1825] between any given HARP pair in a set of HARP peers. The HARP pair may use a TCP connection between them at boot for route synchronization, and will use UDP to forward Mobile-IP registration packets. It is required that all of these end to end TCP and UDP channels be protected by at least IPSEC authentication [RFC 1826], and optionally by authentication and encryption [RFC 1827]. Authentication is a requirement. Thus security will be end to end for the HARP protocol between HARP peers.

References

[RFC-826] Plummer, D., "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addresses for Transmission on Ethernet Hardware", STD 37, November 1982.

[RFC-1721] Malkin, G., "RIP Version 2 Protocol Analysis", November 1994.

[RFC-1825] Atkinson, R., "Security Architecture for the Internet Protocol", Naval Research Laboratory, July 1995.

[RFC-1826] Atkinson, R., "IP Authentication Header", August 1995.

[RFC-1827] Atkinson, R., "IP Encapsulated Security Payload", August 1995.

[RFC-2002] Perkins, C., "IP Mobility Support", October 1996.

[RFC-2003] Perkins, C., "IP Encapsulation within IP", October 1996.

[RFC-2178] Moy, J., "OSPF Version 2", July 1997.

Contacts

Bjorn Chambless
Computer Science Department
Portland State University
Email: bjorn@cs.px.edu

Jim Binkley
Computer Science and Engineering Department
Oregon Graduate Institute
Email: jrb@cse.ogi.edu