Mobile-IP Priority Home Agents for Aerospace and Military Applications

William D. Ivancic, NASA/GRC
David H. Stewart, Verizon/GRC
Phillip E. Paulsen NASA/GRC
Terry L. Bell, Lockheed Martin/GRC
NASA Glenn Research Center
Cleveland, Ohio 44135
(216) 433-4000
First.M.Last@grc.nasa.gov

Dan Shell
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706
(216) 643-2422
dshell@cisco.com

Abstract—Recent developments in mobile router technology include the ability to prioritize selection of the home agent by the mobile unit. This technology was originally developed for route optimization. However, the technology also can be applied to autonomous catastrophic recovery, and robust redundant network control centers. This paper describes a variety of architecture scenarios that can benefit from prioritized home agents including: homeland security, virtual mission operations, mobile command centers and route optimization for aeronautical applications. A demonstration testbed will be presented where this technology was proven in the field. In addition, a virtual mission operation center demonstration currently being deployed will be described.

TABLE OF CONTENTS

1. INTRODUCTION

NASA Glenn Research Center and Cisco Systems have been performing joint research on mobile networking technology under a NASA Space Act Agreement. As part of this joint research, a number of mobile networking architectural concepts have been investigated that directly apply to the United States Government's National Security Space Architect (NSSA) Transformational Communication Architecture (TCA) as well as the National Airspace System (NAS) [1]. Of particular interest are those architectures that address catastrophic recovery of command and control centers, mobile command and control centers, and route optimization of mobile networks.

2. MOBILE-IP

Mobile-ip is a routing protocol that allows hosts (and networks) to seamlessly "roam" among various IP subnetworks. This is essential in many wireless networks. Mobile-ip can be useful in wireless networks were the mobile-node's point of attachment to the network is changing due to varying conditions in the wireless medium, even if the mobile-node is not physically moving. Mobile-IP can also be used in a wired network where the mobile-node simply wishes to maintain its network identity as the mobile-node is always contacted through association of its home IP address.

This paper concentrates on deployment of mobile networks using mobile-ipv4 [2]. In mobile-ipv4, there are four basic

[2] IEEEAC paper #1317, Version 2, Updated December 15, 2003

elements in mobile-ip, the home-agent, the foreign-agent or access router and the mobile-node.

"The home-agent (HA) is a router on a mobile-node's home network that tunnels datagrams for delivery to the mobile-node when it is away from home, and maintains current location information for the mobile-node.

The foreign-agent (FA) is a router on a mobile-node's visited network that provides routing services to the mobile-node while registered. The foreign-agent provides a temporary address to the mobile node, the care-of-address and detunnels and delivers datagrams to the mobile-node that were tunneled by the mobile-node's home-agent. For datagrams sent by a mobile-node, the foreign-agent may serve as a default router for registered mobile-nodes."

An access-router is similar to a foreign-agent router in that it provides a temporary address to the mobile node, the collocated-care-of-address, and is the first node of connectivity back to the home-agent. However, the access-router does not detunnel the datagrams. Rather, that portion of the foreign-agent function is performed by the mobile-node using the collocated-care-of-address. Note, foreign-agent routers do not exist in mobile-ipv6, only access-routers do. All ipv6 nodes use collocated-care-of-addressing.

"The mobile-node (MN) is a host or router that changes its point of attachment from one network or subnetwork to another. A mobile-node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available."

3. PRIORITY HOME AGENT

The Priority Home Agent (HA) is currently a Cisco Systems vendor specific option for mobile-ipv4 and utilizes the Mobile IP Vendor/Organization-Specific Extensions [3]

"The priority home agent feature changes the behavior of the HA priority configurations on the mobile router without adding any new commands. Each HA will have an access list containing all the foreign agent care-of addresses in its region. When a mobile router sends a registration request to the best HA, the HA will accept or deny the request depending on which care-of address is used in the registration request. If the HA denies the request because the care-of address is not in the access list of that particular HA, the mobile router will try to register with the next best HA, and so on. If HAs have the same priority, then the most recently configured HA takes precedence. If registration with even the lowest priority HA fails, the mobile router will wait for an advertisement and then try to register again starting with the highest priority HA. When the mobile router registers with a new HA, it will also attempt to deregister with the old HA using the old foreign agent care-of-address[4]."

The HA priorities are set in the configuration settings in the mobile router (MR). The MR will attempt to register with the highest priority HA. Two possible scenarios will occur: If no response is received from the highest priority HA after three attempts, the MR will attempt to register with the next highest priority HA. If the HA sends a request denied message to the MR, the MR will immediately attempt to register with the next highest priority HA. The former provides a mechanism for disaster recovery whereas the latter is useful for route optimization.

4. ARCHITECTURAL CONCEPTS

In this section we describe three basic architectural concepts that utilize mobile networks and prioritized home agents. These concept address route optimization, catastrophic recovery and command on the move.

Route Optimization

Priority HA was originally conceived to address route optimization. Prioritized HA is synonymous with geographically distributed HAs and reparenting of the HA.

For mobile-ipv4 deployments across public infrastructure or when considering corporate security policies, reverse tunneling is almost always required. As such, all traffic must pass through the HA due to ingress filtering, NAT transversal, or security policy. No route optimization is possible, not even triangular routing. Priority HA is a technique that improves route optimization by allowing the "best" HA to be utilized. Here, "best" generally means most geographically desirable.

Consider an aeronautics example. A fictitious airline company, ACME, operates globally with most of its traffic in the United States, Europe, or Asia. Its main headquarters and associated HA is in the United States. Additional regional offices are located in Paris, France and Beijing, China. Without prioritized HAs, all traffic, anywhere in the world would have to pass through the HA in the United States. An ACME aircraft that has landed in France will have all its network traffic tunneled back to the US.

Assume prioritize HAs are deployed in each regional office with the following priority from highest to lowest: US, Paris, Beijing. Now, consider the ACME aircraft is communicating over satellite with the ground station in Munich Germany. The MR will attempt to register first with the US HA and will get a request denied. The MR will immediately attempt to register with the Paris HA and be accepted. Now all traffic is simply tunneled between the

aircraft and Paris. Route optimization (to the extent currently possible) is achieved.

Catastrophic Recovery

Mobile-ip and the use of prioritized home agents provides a mechanism for addressing catastrophic recovery from network disasters resulting form natural or man-made catastrophes.

Many networks are configured in a hub/spoke architecture as shown in figure 1. A primary control site may become physically inaccessible for a number of reasons such as a health quarantine or hostage situations. However, these sites may be electronically accessible via connections to a secondary site. In this scenario, the system can be controlled remotely, and no communications is lost. Mobile-ip is not needed here. However, if for some reason, the primary control site becomes physically incapacitated, all communications is lost.

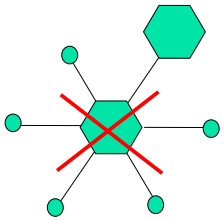


Figure 1 - Hub/Spoke Architecture

By implementing a fully meshed network and deploying prioritized home agents, a control network can be constructed that is robust enough to handle the catastrophic loss of its primary control center due to war, terrorist attacks or natural disasters [Figure 2]. In this scenario, if a mobile unit cannot register with its primary HA, it will attempt to register with the next HA in its prioritized list. Here, the HAs are not being utilized for route optimization, but rather for redundancy. Therefore, the HAs do not have access lists configured to deny particular mobile networks.

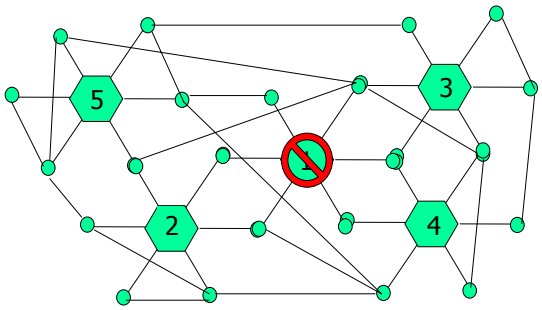


Figure 2 - Meshed Network

Command On The Move

The same techniques used in the case of catastrophic recovery can be deployed in a military setting for command on the move. Figure 3 illustrates such a case. During normal operations, all communications passes through the primary HA which has reach back connectivity to the Intelligence control center via a satellite link. When the situation arises where it becomes necessary to move the command center, a secondary HA can take over while the primary moves. In this manner, communication between the battle group command center and the troops is maintained while the primary command site is redeployed at a new location. Once redeployed, connectivity to the primary will established and the secondary can be redeployed to the new location. Thus, connectivity to the troops is maintained during the entire jump operation.

5. PLUM BROOK DEMONSTRATION

To fully test the priority HA feature related to geographically distributed HAs, a field test and demonstration took place at NASA's Plum Brook facility in June of 2003. Plum Brook is a facility that encompasses approximately 9000 acres of land in Sandusky, Ohio. The

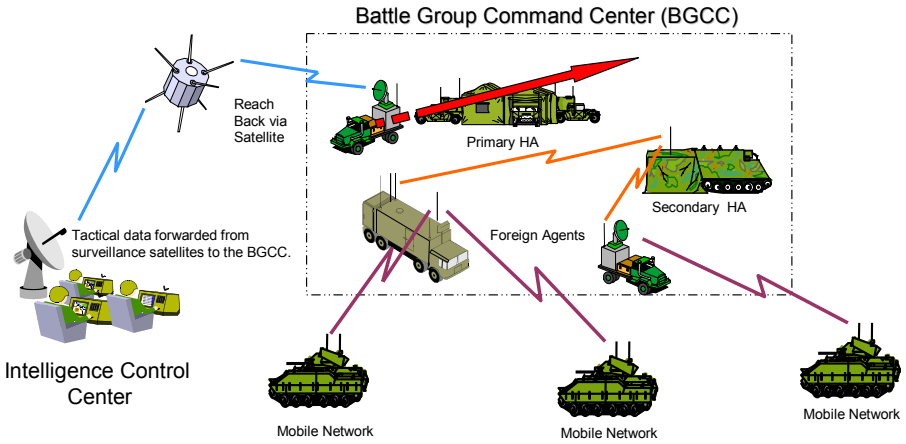


Figure 3 - Command On The Move

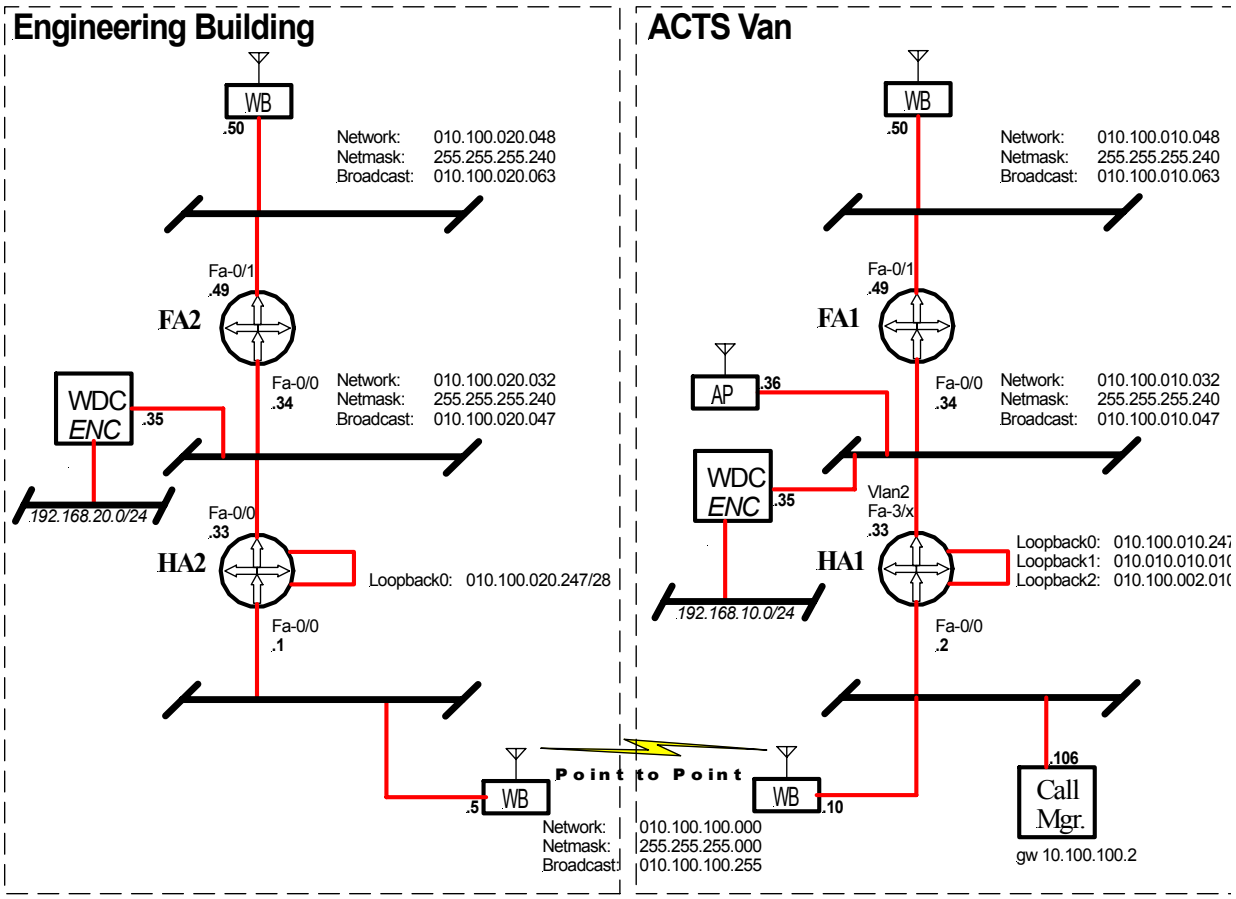


Figure 4 - Plum Brook Network Backbone

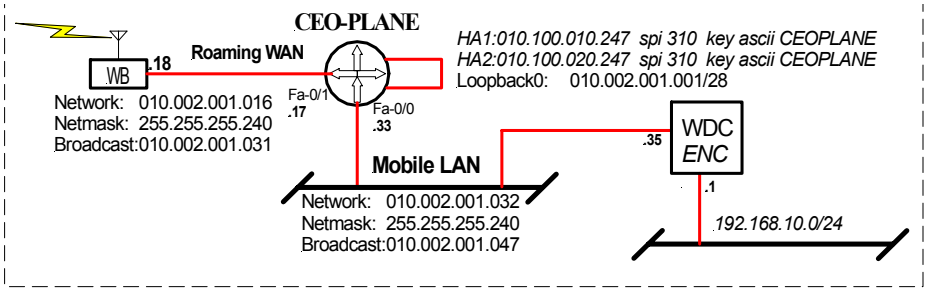


Figure 5 - Mobile Network

Plum Brook facility is crossed with a number of small roads and provides a diversity of terrain and foliage to enhance our network testing with some practical RF system evaluation – particularly relative to 802.11b at 2.4 GHz.

Figure 4 shows the backbone topology that was used to demonstrate the Mobile Router's (MR) Priority HA Assignment feature [4]. The topology shows two sets of Home and Foreign Agents (HA1, FA1 & HA2, FA2) geographically separated with a wireless point-to-point link connecting them. In this particular scenario, HA1 has an access list of care-of-addresses (COA) that are to be permitted registration request from FA1 and deny a registration request from FA2. HA2 has a similar access list that permits registration for FA2 and denies registrations from for FA1's COA. Assume a mobile router (MR) has its home agent priority list as HA1 followed by HA2. Assume the MR was previously registered with HA1 through FA1 and has now moved such that it can no longer connect to FA1, but can connect to FA2. When the MR attempts to register to its HA through FA2, it will first send a registration request to its highest priority HA, HA1. HA1 will deny the request because the COA used does not correspond to one that is accepted by HA1. The mobile router will try to register with the next highest priority HA, HA2 and will be successful. Thus the MR is now registered to an HA that is geographically much closer. Once the mobile router has successfully registered with HA2, it will attempt to deregister with HA1 using the old foreign agent COA

In this particular network scenario, we implemented three separate mobile networks. Figure 5 illustrates one of these networks. There are two interfaces on this particular mobile router. Only one is configured for roaming and provides the wide area network (WAN) interface connectivity via an 802.11 link. The second interface is the mobile local area network (LAN). One could have multiple mobile LANs and multiple roaming interfaces. However, for this demonstration, implementing one WAN and one LAN was sufficient.

We also demonstrated secure mobile networking. The protected (red) networks are behind Internet Protocol Encryption units provided by Western Datacom (IPE-2M) [5]. These units were developed to be used independently or integrate with the Cisco Systems 3200 mobile access routers. As such, they provided a very small package for the mobile units. In figures 4 and 5, the protected Networks are:

102.106.10.0/24 (Protected LAN off of HA1)
102.106.20.0/24 (Protected LAN off of HA2)
192.168.10.0/24 (Protected mobile LAN off MR1)

Any hosts residing on the black (unprotected) network could not correspond with any hosts on the red (protected) network and visa versa.

Note, there is a wide area network point-to-point link established between HA1 and HA2. This was done to enable deployment of Voice-Over-IP as the call manager was located in the same location as HA1. Thus in order for a VOIP phone to operate properly, it needed reachback to the call manager weather the VOIP mobile network was registered to HA1 or HA2.

6. VIRTUAL MISSION OPERATIONS CENTER

NASA is working with Cisco Systems, General Dynamics and the various organizations within the United States Department of Defense to implement a virtual mission operations center (VMOC) using Internet technologies. A cornerstone of the current architecture is deployment of prioritized HAs.

The current concept is being directed at command and control of space systems. Current command and control centers have to be manned 24/7. This is also the case for the backup command and control centers. Deployment of the VMOC will drastically reduce the people needed to manage the center and allow that management to take place remotely. Thus, if a primary command center becomes physically disabled; the secondary could automatically take over and be controlled by the same operator who controlled

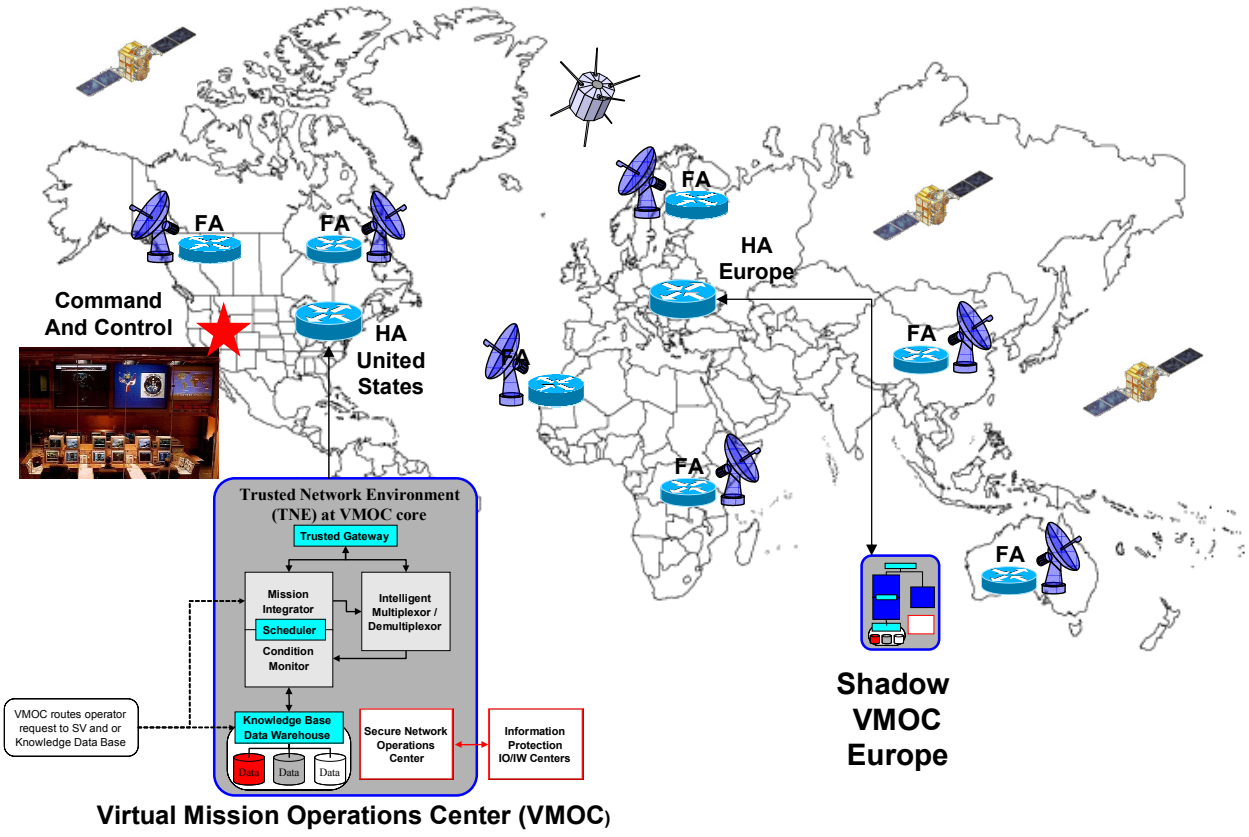


Figure 6 - Virtual Mission Operations Center

the primary. This architecture requires that the primary and secondary command centers' data bases to be synchronized and for the mobile assets, to automatically know when the primary control center went down and the secondary took over. The later is possible by deployment of prioritized home agents.

Figure 6 illustrates the network concept. Consider the space assets are low earth orbiting (LEO) satellites that can communicate with numerous ground stations spread throughout the world. We have two VMOCs available to control the assets. One is located in the US and the other in Europe. The US VMOC is primary. Since we wish either VMOC to be utilized by the space assets, but prefer them to use the US VMOC, no access lists are implemented in the VMOC Home Agents. However, priority lists are still configured in the space assets mobile routers with the US VMOC given higher priority. As the space assets communicated with various ground stations, they would register to the US VMOC and normal mobile-ip communication would commence. If something happened to the US VMOC, the MR on the space asset would not receive a reply from the primary HA. There would be no "deny" message either. Thus, the MR would attempt to register with the US VMOC two more times prior to registering with the VMOC in Europe. These retry attempts may take 30 to 90 seconds per try depending on the retry timer configuration. For assets such as LEO spacecraft such registration times are significant considering a satellite may only be in view of a ground station for a few minutes. Thus, having more than two or three VMOCs configured in the MR may be impractical although having multiple VMOC on the ground is quite reasonable.

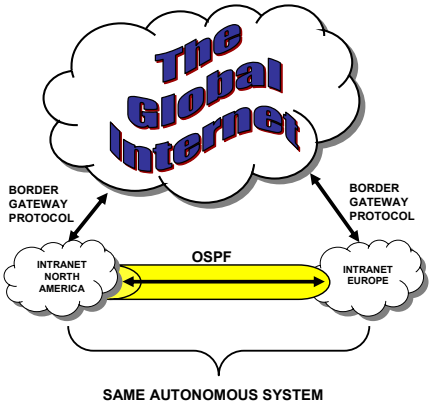


Figure 7 - Interconnecting Geographically Distributed Dynamic Home Agent

Once registration occurs with a secondary VMOC, it may be beneficial to reconfigure the priority lists in the mobile units to make this new VMOC the primary. Otherwise, the mobile units will always attempt to register with the VMOC that is out of commission. This will result in reduced system performance due to the number of registration retries and the length between registration retries.

7. Potential Problems / Issues

For certain network architectures such as the virtual mission operations architecture, the number of registration retries and time between retries are critical parameters effecting system performance. It is highly desirable to make these settable parameters.

The various prioritized home agents must be in the same autonomous systems (AS) in order to ensure that mobile routes are not advertised by multiple HAs without the proper weighting. A more defined route will receive greater weight. However, if a mobile router is isolated; multiple HAs may advertise the route with duplicate weight. This can be handled by internal gateway protocols.

If HAs within an autonomous system are physically separated by long distances (i.e. Europe and United States) and correspondence occurs between mobile networks and hosts utilizing the open Internet, then the AS should have multiple connections to the open Internet. Otherwise, all traffic from the open internet will have to enter via a specific location thereby reducing the effectiveness of route optimization via priority home agents.

Figure 7 illustrates geographically distributed home agents. Assume one home agent is located in North America and the second in Europe. One would want a connection for the autonomous system (AS) to the global Internet in both Europe and North America. If the only connections to the AS were in North America, all traffic to either HA would have to flow through that connection defeating the purpose of geographically distributed home agents. In addition, the home agents must be able to communicate with each other through the autonomous system's network using common routing protocols and policies.

8. Migration toward IPv6

Work is ongoing regarding mobile networking using mobile-ipv6 in the Networks in Motion (NEMO) working group of the Internet Engineering Task Force (IETF) [6]. Much of the basic operations in the NEMO Basic Support is closely based upon work and lessons learned with mobile network deployments in ipv4. In particular, route optimization that is normally associated with mobile-ipv6 is not performed in the NEMO Basic Support draft. Rather, bi-directional tunneling is performed similar to that found in ipv4 reverse tunneling using collocated care of addresses. However, route optimization is expected to be address in NEMO once the basic implementation is completed.

The basic specification for mobile networks using ipv6 is currently in development and interoperability testing. The final specification is anticipated to be completed by the end of 2004. Once the basic specification is completed, the NEMO group may recharter to address route optimization issues related to mobile networking.

Work is ongoing in transitioning to mobile networks using mobile-ipv6 while still maintaining compatibility with existing ipv4 networks as ipv4 network are expected to remain in existence for many years. An example of such "work in progress" includes IPv4 traversal for MIPv6 based Mobile Routers [7].

Ipv6 work is taking place which is similar to the prioritized home agents concepts for ipv4. This work is in the form of an Inter Home Agents protocol. The proposed Inter Home Agents protocol is relevant to both mobile-ipv6 protocols and the NEMO basic support protocols. It provides Home Agent redundancy and load-balancing for both protocols. The Inter Home Agents protocol allows multiple Home Agents to be placed at different links. It also allows a Mobile Node/Router to utilize multiple Home Agents simultaneously [8].

9. SUMMARY

The priority home agent feature was originally conceived to help alleviate route optimization problems for mobile networks using mobile-ipv4. This feature can also be deployed to improve system robustness and for military command on the move and virtual mission operation centers. Experience gained in future deployments will aid the IETF Networks in Motion working group in specifications for ipv6 mobile networks.

10. REFERENCES

[1] http://www2.faa.gov/nasarchitecture/hilites/index.htm, October 2003

[2] C. Perkins, "RFC3344 - IP Mobility Support for IPv4," August 2002

[3] G. Dommety, K. Leung, "RFC3115-Mobile IP Vendor/Organization-Specific Extensions," April 2001

[4] Cisco Mobile Networks—Priority HA Assignment Cisco IOS Release 12.2(15)T), October 2003

[5] http://www.western-data.com/, October 2003

[6] http://www.ietf.org/html.charters/nemo-charter.html, October 2003

[7] P. Thubert, M. Molteni, P. Wetterwald, "IPv4 traversal for MIPv6 based Mobile Routers" draft-thubert-nemo-ipv4-traversal-01, May 2003 (work in progess)

[8] Ryuji Wakikawa, Vijay Devarapalli, Pascal Thubert, "Inter Home Agents Protocol (HAHA)," draft-wakikawa-mip6-nemo-haha-00, October 2003

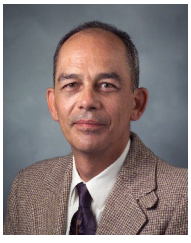
11. BIOGRAPHIES

Phillip E. Paulsen *received a B.S. degree in mechanical engineering and a Masters in Business Administration from Cleveland State University. He is a certified NASA Project Manager with over 14 years of experience in the design and development of space flight systems. He served as the Tracking and Data Acquisition Manager (TDAM) for all intermediate and large class NASA ELV missions from 1993 to 1999. Since 1999 Mr. Paulsen has been managing the development of Internet Protocol-compliant network hardware and software for use in space-based platforms.*

Dan Shell *is a Network Architect for Cisco Systemss Global Defense and Space Group specializing in Wireless, Mobile and Satellite Networking. As the lead engineer in the support of the CISCO/NASA Space Act Agreement for joint network research over high delay and high data rate networks, Shell has been actively involved with NASA Glenn Research Center in researching IP over satellite and Internet nodes in space*

Will Ivancic *is a senior research engineer at NASA's Glenn Research Center working in the networking and advanced communication technology development. Mr. Ivancic's work includes: advanced digital and RF design, communications networks, satellite onboard processing, and system integration and testing, Mr. Ivancic's recent work has concentrated on research and deployment of secure mobile networks for aerospace and DoD networks*

David Stewart *is a communication engineer at Verizon. David specializes in RF and wireless communication networks. His current work involves development and deployment of secure mobile networking technologies in various testbeds at NASA's Glenn Research Center, as well as deployment of early-field-trial aeronautic and maritime mobile-networks.*



Terry Bell *is a network and telecommunication engineer for Lockheed Martin Global. His responsibilities include support of advanced protocol research for space and aeronautical based networks at Glenn Research Center. He is currently involved in research and early field deployment of secure mobile networks using IPv4 and IPv6 technologies.*