NASA/TM—2008-215065

IEEEAC Paper no. 1071, Version 1

Problems With Deployment of Multi-Domained, Multi-Homed Mobile Networks

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

April 2008

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to *help@sti.nasa.gov*

- Fax your question to the NASA STI Help Desk at 301–621–0134

- Telephone the NASA STI Help Desk at 301–621–0390

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/TM—2008-215065

IEEEAC Paper no. 1071, Version 1

Problems With Deployment of Multi-Domained, Multi-Homed Mobile Networks

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

Prepared for the
2008 Aerospace Conference
cosponsored by the IEEE and AIAA
Big Sky, Montana, March 1–8, 2008

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

April 2008

Acknowledgments

The author would like to thank Terry Bell, Wesley Eddy, David Stewart and Terry Davis for their review and comments.

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Available electronically at http://gltrs.grc.nasa.gov

Problems With Deployment of Multi-Domained, Multi-Homed Mobile Networks

William D. Ivancic
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Abstract

This document describes numerous problems associated with deployment of multi-homed mobile platforms consisting of multiple networks and traversing large geographical areas. The purpose of this document is to provide insight to real-world deployment issues and provide information to groups that are addressing many issues related to multi-homing, policy-base routing, route optimization and mobile security – particularly those groups within the Internet Engineering Task Force.

TABLE OF CONTENTS

1. Introduction

The purpose of this document is to provide insight into real-world deployment issues and provide information to working groups that are addressing many issues related to multi-homing, policy-based routing, route optimization and mobile security.

This document describes numerous problems associated with deployment of multi-homed, mobile platforms consisting of multiple networks in multiple domains and traversing large geographical areas. These multi-networked, multi-homed, multi-domained mobile networks are often large platforms such as planes, trains, or ships and even automobiles and spacecraft. One key characteristic that separates them from general "networks in motion" (NEMOs) is that these platforms have multiple networks that are generally owned and operated by different parties (domains). Because of the various network domains, policy-based routing and security have some different issues and concerns relative to single-domained systems.

Three examples of multi-domained, multi-networked systems include: defense, aeronautics and space. In all of these environments there are critical control systems that reside in a particular network which require highly reliable links and time-critical information, but limited bandwidth. We shall call this network the "command and control" domain. A second network may be present for operations and maintenance. This "operations and maintenance" domain requires little bandwidth. In addition, information is not as time-critical and reliability is relaxed. The third network is the "user domain". This network generally requires much more bandwidth than does command and control network or operations and maintenance. However, this network, to date, has generally not required data to reach its destination within a guaranteed time.

In the aeronautical industry, all critical air traffic control (ATC) is performed via a closed network. Currently the air/ground link is not Internet-based, but this is expected to change in the future. All ATC traffic is time-critical and the links must be highly reliable. However, these links require relatively little bandwidth in the order of 10s of kilobits per second. This domain, to date, has been a closed network with all infrastructure effectively owned or controlled by the civil air authorities. In the United States of America, this civil air authority is the Federal Aviation Administration (FAA).

The second domain is used for aircraft operations and maintenance and is call the airline operational communications (AOC) network. Information that may run on this network includes passenger lists, aircraft fuel and weight and other operations and maintenance information. This link is not as safety critical and the information carried over this link is generally not time-critical. Like the ATC domain, the AOC domain is closed. To date, this network has resided within the same closed network as ATC as AOC has paid for much of the technologies use by ATC.

The third domain is the passenger domain. This domain is used for in-flight entertainment (IFE) services and communication. To date, the IFE network has not been allowed to carry any time critical ATC communications. This policy is in place in part for security and in part because the IFE network has not been specified and certified to the same time-critical information transfer and reliability as the ATC network. However that does not imply that the IFE network could not meet those requirements.

A second example of multi-domained, multi-networked systems is the deployment of Internet technologies for the United States National Aeronautics and Space Administration (NASA) space program. Three domains of interest for a spacecraft are: ground operations located in Florida; mission

control located in Texas; and the general science community. Both ground operations and mission control require reliable, time-critical commanding but do not require large amounts of bandwidth – assuming video is sent on its own links. The user network (scientific community) has greatly relaxed reliability requirements and do not require time-critical information. However, the user network is expected to transport large volumes of data. Each of these networks is effectively owned and operated by a different community of interest on different domains.

Other multi-domained, multi-networked systems might be found in military operations, the global shipping industry, taxi and limousine services, and perhaps even in the general automotive industry.

2. Mobility Solution Space

Mobility here is the ability to move between radio systems and networks without having to reestablish sessions. Mobility can be performed as a host-based or network based solution. Mobility can also be performed at various layers including the radio-link, transport and network layers. Two network layer technologies that are applicable include routing protocols or Mobile-IP based solutions such as NEMO.

Host-Based Solutions

Host-based solutions include: SCTP [RFC3286] at the transport layer, HIP [RFC4423] as a shim between the network and transport layers and Mobile-IP at the network layer [RFC3344] [RFC3775]. A major problem with host-based solutions occurs when a large number of hosts are sharing the same low-rate radio link. A binding update storm will occur when a network is traversed. All hosts have to inform all of their corresponding nodes as well as their location managers (e.g., home agent for Mobile-IP, DNS or some other location manager for SCTP, and rendezvous servers for HIP) when their location has changed. This can saturate the RF link. Thus host-based solutions have a scalability problem for this situation.

Radio-Link Layer Mobility

Radio-link layer mobility is currently deployed in cellular systems and works effectively over relatively large geographical areas (i.e., countries and continents). Use of radio-link handoffs for mobility provides a partial solution over a limited space. Radio-link layer handoffs only solve mobility problems for a single link. It does not address multihoming nor is it scalable over extremely large geographic areas (i.e., globally). Since multiple providers, possibly with multiple access link technologies, are usually required for global connectivity, link-layer mobility solutions alone are not feasible for global mobility.

Transport Layer Mobility

Transport layer mobility using Stream Control Transport Protocol (SCTP) provides route optimization and potentially could provide good convergence times. As with any non-routing protocol, transport layer mobility requires some sort of location manager to enable a corresponding node to initiate communications. The location manager is used by the mobile node to register its current location. Use of Domain Name Servers (DNS) has been shown to functionally perform this function using “do not cache” options. However, the reliability and convergence time for updating the DNS has not been proven operationally as often times the “do not cache” option is ignored [Pan2004].

SCTP-based transport layer mobility and has been implemented as a host-based solution. This solution currently is not applicable for large mobile networks. However, research is being performed to use one-to-one address translation to provide network-based SCTP whereby one host acts and an SCTP proxy for all hosts behind it performing SCTP for all hosts behind it. Conceptually this effectively performs transport-layer mobile routing. However, even if SCTP can be adapted to handle many nodes, binding update storms may still be a problem.

Routing Protocols for Mobile Networks

Routing protocols provide route optimization as that is their job. There are a number of problems with using routing protocols to solve the multi-domained, multi-homed mobile network problem including: convergence time, inability to share network infrastructure, addressing, scalability and the applicability of some routing protocols for particular applications.

Figures 1 and 2 illustrate some of the major issues with using routing protocols for mobile networks. Figure 1 shows how the current International Organization for Standardization (ISO) standards based Aeronautical Telecommunication Network (ATN) as specified by the International Civil Aviation Organization (ICAO). Figure 2 shows a conceptual migration to use of internet protocols (IP) to perform the same function.

For mobile networks that require time-critical command and control, fast convergence time is essential. Take, for example, the ATC problem with aircraft takeoff and landing. This is the most crucial portion of a flight. One cannot wait 30 to 90 sec or a few minutes for routes to converge. The same is true for a spacecraft during launch when it is passing numerous ground stations in a short time. In order to control the convergence time in aeronautical networks, the ISO Inter Domain Routing Protocol (IDRP) is used [ISO10747]. To further improve convergence time, the network is constructed as a highly controlled two tier architecture consisting of transit routing domains and backbone interconnectivity. The concept

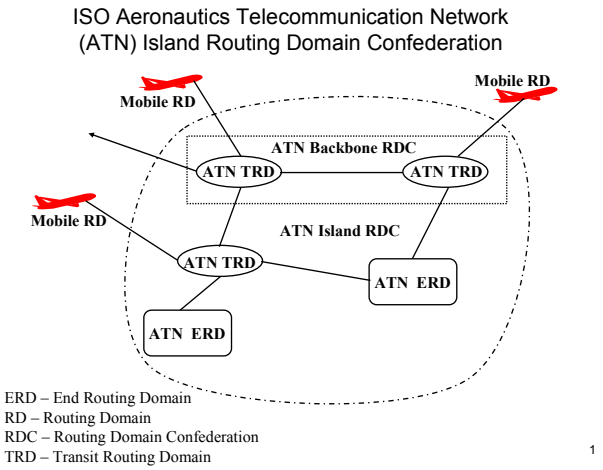

Figure 1.—Aeronautical Telecommunication Network Island.

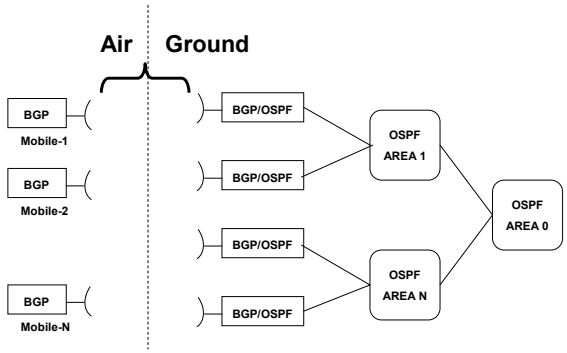

Figure 2.—Internet Protocol Based Aeronautical Network.

is that route propagation will occur quickly in the transit-domain where information is time-critical [Sig1998]. Route propagation to geographically distant areas will occur over the backbone where route propagation is not time-critical (fig. 1).

In the IP implementation of figure 2, BPG-4 [RFC4271] is seen as an external route to the OSPF network [RFC2328]. Since the aeronautics network is relatively small and currently a closed network operated jointly by various civil aviation authorities, OSPF can be used globally. When a BGP route is advertised to the OSPF network, the OSPF network will immediately propagate the route into the nearest OSPF area thereby provide good convergence time locally where it matters most [Iva2006].

In figures 1 and 2, IDRP and BGP are also used to provide policy-based routing capability. This is of interest and a current requirement for the aeronautics community in order to have time-critical command and control flow through one link while other traffic such as air operations flows through another. Although this requirement has existed within the ICOA ATN specification from the beginning [ICAO9739] [ICAO9705], its use has seen limited deployment to date and is operationally untested for the following reasons: there currently are not enough ATN users to tax the system; system deployment is minimal; and, the airlines generally only have one link active for cost reasons. For example, satellite links are not turned on unless needed due to the high cost. Furthermore, two simultaneous VHF radios are not active simultaneously.

When using BGP or other routing protocols for mobility, additional problems arise due to addressing. Routing protocols generally assume the interface connections on the routers are not dynamically changing. Thus, two routes connected are assumed to be on the same subnet. One may be able to use "un-numbered" serial interfaces to alleviate this problem, but to date, this has not been proven to work. Thus, all mobile platforms must reside in the same network or sub-network for IPv4. It may be possible to achieve this by having the mobile platform obtain its WAN interface address from the ground using PPP, DHCP, or IPv6 auto configuration. Note, for IPv6, routers do not have to reside on the same subnet is routing information is exchanged over the link-local address, not the global address. This is an extremely attractive feature and differentiator between IPv4 and IPv6.

Regarding use of an inter-autonomous system protocol such as BGP, scalability issues arise due to the need to configure peering. Each BGP router has to have a configuration for each autonomous system (AS) peer that wishes to communicate with. Thus, each mobile has to be preconfigured for each radio station router it will communicate with. Likewise, each radio station router will have to be preconfigured for each mobile. As the number of ground stations or mobile platforms grows, this quickly becomes unmanageable. As new mobile platforms or ground stations are added, all configurations must be updated. Furthermore, if the mobile platforms have multiple-domains, the question of who is authorized to update systems becomes an issue.

Using general routing protocols for mobility makes it very difficult to share infrastructure. In order to run routing protocols, one generally has to either own all of the assets or pre-arrange peering agreements. For security reasons, one cannot simple inject routes into another's network. Furthermore, allowing relatively small mobile networks to inject routes that do not conform to some form of route aggregation will result in route table explosion and is therefore not scalable or desirable.

NEtworks in MOtion (NEMO)

Networks in Motion (NEMO) protocols have been designed specifically to manage the mobility of an entire network (or networks), which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology [RFC3963]. NEMO protocols also address multihomed networks which may be either a single mobile router (MR) that has multiple attachments to the internet, or may use multiple MRs that attach the mobile network to the Internet.
NEMO protocols, by design, avoid many of the problems associated with using general routing protocols for mobile networks including: convergence time, the need for two

communicating routers to reside on the same subnet and the need to pre-configure peering relationships.

Mobile-IP based solutions such as NEMO solutions have relatively fast convergence times as Mobile-IP based protocols simply redirecting the default-route pointer. However, if one wishes to pass routing protocols down a Mobile-IP tunnel, then convergence issues may still exists.

NEMO solutions also allow one to easily share communication infrastructure. NEMO solutions do not require the mobile to inject routes into another's network. Rather, for each radio link one simply contracts with an Internet Service Provider (ISP) for bandwidth and access. The ISP provides a care-of-address once radio-link access is granted. The user can use the bandwidth however they wish. (Note, this model may change if mobile network users dominate use of the IPS's network. At that point, the cost model may change whereby a mobile network user pays an appropriate usage fee relative to the capacity used.)

Two areas that NEMO protocols have yet to mature in are support for route optimization and policy-based routing.

Current NEMO support requires a bi-directional tunnel between the mobile router and the home agent. This can result in significant delays when the mobile unit traverses large distances. These distances can be global distances (or beyond for space systems). It is highly desirable to have route optimization at least to the point of being able to bind a mobile node to a geographically closer home agent. Route optimization is expected to be the next area of work being performed by the Internet Engineering Task Force (IETF) via the Mobility EXTensions for IPv6 (MEXT) working group.

Another area of route optimization relative to Mobile-IP and NEMO is network-based local mobility management (netlmm). Local mobility involves movements across some administratively and geographically contiguous set of subnets. When a mobile node moves from one access router to another, the access routers send a route update to the mobility anchor point. While some mobile node involvement is necessary and expected for generic mobility functions such as movement detection and to inform the access router about mobile node movement, no specific mobile node to network protocol will be required for localized mobility management itself. Netlmm technology may prove useful for common radio systems owned and operated by a single entity. In the aeronautics community, netlmm may be useful for connecting all of the VHF radios in a given control area. For a space mission, netlmm between tracking ground stations may greatly improve performance for time critical commanding.

Past implementations of NEMO IPv4 or IPv6 protocols only allow for binding to one care-of-address. In this situation, a multihomed mobile router can only use one link at a time. It is not capable of using two or more links even if they are available. Use of multiple links simultaneously is desirable for a number of reasons including load balancing and policy-base routing. The problem of policy-base routing was being investigated by Mobile Nodes and Multiple Interfaces in IPv6 (monami6) working group. That work is being transitioned to the MEXT working group as monami6 is combining with the Mobile-IPv6 and nemo working groups. Two topics being investigated that of interest to multi-domained, multi-homed mobile networks are:

- A protocol extension to Mobile IPv6 (RFC 3775) and NEMO Basic Support (RFC 3963) to support the registration of multiple Care-of-Addresses at a given Home Agent address [Wak2006].
- A "Flow/binding policies exchange" solution for an exchange of policies from the mobile host/router to the Home Agent and from the Home Agent to the mobile host/router influencing the choice of the Care-of Address and Home Agent address [Sol2006].

3. Policy-Based Routing

Figures 3 through 5 illustrate the advantages of policy-based routing in a mobile aeronautical network. Consider the mobile network having three links available. One link is classified as highly reliable but relatively low rate. This link is reserved for command and control. The second link is a low-latency, low-bandwidth link. The third link is high-rate for passenger services. Assume it is possible to set policy with the following rules:

- Only ATC traffic is allowed to use the reliable link.
- Data precedence is set such that ATC is highest priority, AOC is next highest and passenger traffic has lowest priority.
- ATC and AOC traffic are allowed to use the low-latency link.
- ATC, AOC and passenger traffic are allowed to use the high-rate link.
- Link preference for ATC is reliable link – highest, low-latency link – middle, high-rate – last.
- Link preference for AOC is low-latency followed by high-rate.

Figure 3 shows all links active. Figure 4 shows that ATC traffic can be delivered even if all other links are unavailable. Figure 5 shows that ATC and AOC traffic have precedence over passenger traffic and could use the high-rate link if their preferred links are unavailable. Figure 5 is of greatest interest because one could conceivably make this the preferred link for all traffic if safety-of-flight QoS requirements could be met.

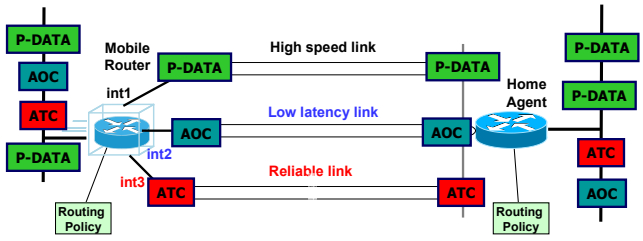

Figure 3.—Policy-Based Routing, All Links Active.

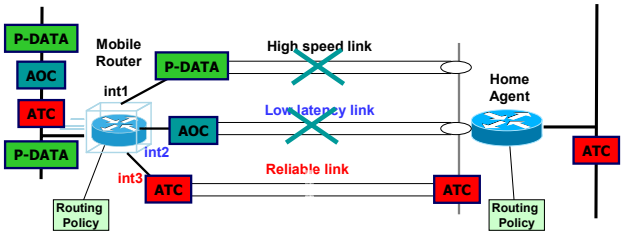

Figure 4.—Policy-Based Routing, Critical Link Active.

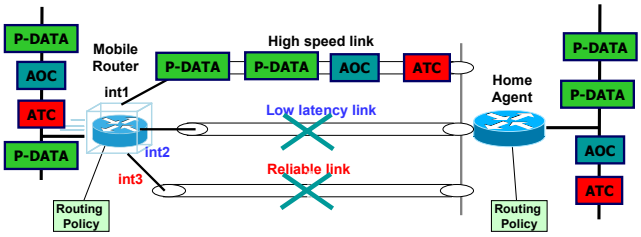

Figure 5.—Policy-Based Routing, Passengers Link Active.

Doing so would release spectrum to ATC and AOC as many users could be using the high-rate links when available. (For aeronautical communications, RF spectrum is a precious and limited resource.)

4. Radio Operations

Mobile networks may utilize many types of radio systems. It is imperative to understand the interaction between particular radio systems and the routing and transport protocols. For example, the Transmission Control Protocol (TCP) has algorithms to enable it to probe the network for capacity and adjust accordingly. Streaming video or rate-based protocols do not and can easily saturate a link if not properly controlled. Two techniques that can be used to control non-congestion-friendly protocols are policy-base routing and queue management.

Layer-2 Triggers

For low rate (10s of kbps) radio links such as current avionics links, some minimal quality-of-service can be accomplished via message prioritization. When link capacity is low there is little need to have a feedback mechanism between the radio and the router to enhance QoS. Current and future high-rate links would benefit greatly by having a standardized feedback mechanism between the radio systems and the router. Such mechanism could indicate if a link is available and the quality and bandwidth of the link. The former is important for fast handovers between links. The latter is of particular importance for bandwidth-on-demand systems. For instance, the Boeing Connexion outbound radio link was designed to operate from approximately 16 kbps up to 1 or 2 Mbps in 16 kbps increments. The rate was continually varying depending on outbound traffic demands and satellite network congestion. Assuming the interface between the router and Connexion radio is an Ethernet connection, some type of layer-2 trigger or feedback to the router is necessary to determine the available data rate. Otherwise, the router is likely to saturate the radio interface by sending traffic at Ethernet line rates. If the interface is serial, having the radio provide the clock may solve the data rate problem.

Multiplexing Links

When building a robust mobile communication system, it is highly desirable to have multiple radio types to ensure communication (e.g., cellular, WiFi, satellite). Each of these radio link technologies operates at different frequencies and has different antenna technologies that must be incorporated into the system design. Radio systems and their associated antenna systems can add significant size, mass and power to communication systems. Thus, although it is highly desirable to have multiple radio systems, there is a practical limit to what can be deployed. One most certainly does not want to have to deploy multiple radios of the same technology. Rather, one should multiplex communications over similar radios.

Multiplexing at the Radio

Figure 6 illustrates multiplexing communications at the radio link. For each link, all information must be queued and prioritized in the "MUX" box. This is not overly difficult.

One of the main problems with multiplexing at the radios is that the MUX box must obtain or be configured for addressing on the various wireless networks. The MUX box must pass this addressing on to the NEMO routers. For example, the MUX on the WiFi network may obtain its Wide Area Network (WAN) address via DHCP. The MUX must now provide addressing to the various NEMO routers attached to the ingress side. Does the WiFi MUX provide different addresses to each NEMO router or the same address? How is this done? One would like this to be a standardized method.

One advantage that the architecture in figure 6 provides is physical separation of the NEMOs. Thus, security issues for this architecture may be accomplished using a conventional approach. However, if each NEMO is getting the same WAN address, this is certainly not conventional.

Multiplexing at the Router

Figure 7 illustrates combining information in the router rather than a special MUX box per figure 6. Here, multiple NEMOs are configured in a single router. There are many advantages to this architecture over the one in figure 6. First, there is no need for MUX boxes. Second, only one router interface is necessary for each radio system; therefore, traditional forms of acquiring a WAN address can be used (i.e., DHCP, PPP, Auto-configuration, manual configuration) and the same address is not assigned to multiple interfaces.

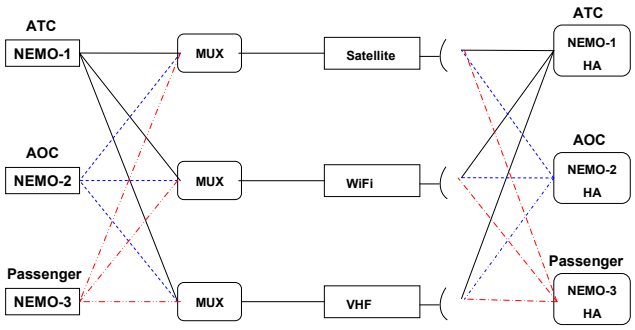

Figure 6.—Multiplexing at the Radio.

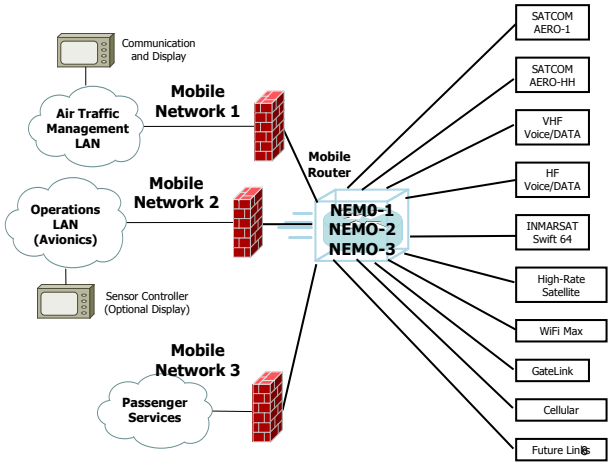

Figure 7.—Multiplexing at the Router.

Third, only one router is required for multiple NEMOs versus use of multiple NEMOs, one for each domain. Thus, there is potential for mass, power, volume and cost savings. Furthermore, this architecture is potentially much easier to manage.

A definite security concern with multiplexing NEMOs and radios at the router is that various domains may be cross connected if configurations are not tightly controlled.

5. Network Access (Auto-Login)

Obtaining access to a wireless network may be non-trivial for a mobile platform, depending on the wireless technology being deployed. A mobile platform should be able to obtain network access in an automated manner.

Cellular Access

For cellular systems, access is usually accomplished via prearranged security and access agreements. A user contracts for bandwidth with a service provider and obtains a cellular modem that has a corresponding electronic serial number. When the modem (phone) makes a call, it transmits the ESN and the Mobile Identification Number (MIN) – also referred to as MSID (Mobile Station Identification) – to the network at the beginning of the call. The MIN/ESN pair is a unique tag for each modem and is used to establish the system's credentials and allow access to the wireless network. PPP or some other protocol can then be used to obtain a care-of-address.

Satellite Access

Satellite radio network access may be performed in a similar manner to cellular radio systems depending on the provider. In some satellite modems a form of electronic serial number or media access control (MAC) address is associated with a modem. Once the ESN (or MAC) is validated, the user obtains access to the network. Network addresses are obtained using PPP or statically configured addresses.

WiFi Access

WiFi radio access is somewhat different than cellular or satellite access. Three basic modes of wireless network access are used: open network, preconfigured and negotiated.

For open networks, any radio simply scans for a radio network and obtains access. Layer-3 address is usually provided via DHCP. Such radio and layer-3 access works well for a machine access (i.e., mobile router access).

A preconfigured access will work for machine-to-machine operations. Such pre-configurations are usually found on private networks. Here, a pre-placed key may be used along with a security protocol such as Wired Equivalent Privacy (WEP) (802.11 encryption protocol). Media Access Control physical addresses may also be configured into access list to limit what radios are allowed to connect to the network.

As security and accountability concerns grow, radio network access is moving toward negotiated access. Here, a user/name and password or some type of token ID and password are required for access. Such secure radio network access techniques include Extensible Authentication Protocol (EAP), and WiFi Protected Access (WPA). Currently such systems focus on the needs of the human mobile user who is in need of short term network access. Machine-to-machine negotiation of radio network access is not part of this operational scenario. Such concepts are new and businesses cases have yet to be considered. For NEMOs to take advantage of WiFi networks, techniques that allow for machine-to-machine radio access without the need for human intervention are imperative.

6. Costs

Although not a protocol issue, the ISP cost model plays a significant role in the ability to deploy large mobile networks especially if they are multi-domained, multi-homed mobile networks. Fixed rate costs for network access is essential to make it viable to budget for a mobile network. Paying a fixed

price for a fixed amount of bandwidth works well as end users can budget for this cost model. If one has to pay by the amount of data that transitions a given network or connect time, it becomes extremely difficult to budget operations. For large-capacity users as it is extremely difficult to project how much data one will transfer over the link from one month to the next. Likewise, if one is being charged for connect time, one needs to deploy a mechanism that only brings a link up when it is needed. This results in a system that is out-bound oriented. Peer-to-peer communications only occurs when the links are turned on. Thus, in order for a corresponding node to initiate communications with the mobile node, some sort of back-channel has to be used to the mobile node to turn on the link of interest.

7. Security Considerations

Having a single router operating in multiple domains either via generic routing protocols or use of Mobile-IP based NEMO protocols has serious security issues. The possibility of having a single mobile router connected to multiple home agents residing in various domains implies that these domains could be inadvertently connected if the mobile router is misconfigured. Similarly, unless great care is taken to configure mobile platform routers that use generic routing, cross-domain connectivity can easily occur.

Management of multi-domain routers is an interesting policy problem. "Who has authority to configure and control the mobile unit?"

ISPs often implement security mechanisms that break NEMO and Mobile-IP. One example of this is deployment of administrative filtering. Here, an ISP may decide to have an out-bound only policy such that all traffic must have originated from within their network. At least one GPRS ISP has such a policy in place. One explanation provided for such a policy is to keep potentially hostile Internet traffic off the network. Probing the GPRS system address space not only posses a threat to customers, but, more importantly steals precious GPRS bandwidth from the users [Iva2003].

References

[ICAO9705] "Manual of Technical Provisions for Aeronautical Telecommunication Network (ATN) - 3rd Edition," June 2002.

[ISO10747] ISO/IEC 10747:1994, Protocol for Exchange of Inter-Domain Routing Information among Intermediate Systems to Support Forwarding of ISO/IEC 8473 PDUS.

[Iva2003] Ivancic, W., "Administrative Filtering," September 2003, http://roland.grc.nasa.gov/~ivancic/papers_presentations/2003/administrative_filtering.pdf.

[Iva2006] Ivancic, W., "Aircraft Mobility using a combination of Internet Standards," ICAO Aeronautical Communications Panel(Acp)Working Group N - Networking Subgroup N1 – Internet Communications Services ACP/WG N/SG N1 Paper 801, May 2006, http://roland.grc.nasa.gov/~ivancic/papers_presentations/2006/ICAO_WG-N_SG-N1_WP-801.pdf.

[Pan2004] Pang, J., Akella, A., Shaikh, A., Krishnamurthy, B., Seshan, S.,"On the Responsiveness of DNS-based Network Control," Proceedings of the Internet Measurement Conference 2004, October 2004.

[RFC2328] Moy., J., "OSPF Version 2," RFC 2328. April 1998.

[RFC3286] Ong, L., Yoakum, J., "An Introduction to the Stream Control Transmission Protocol (SCTP)," RFC 3286, May 2002.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4," RFC 3344, August 2002.

[RFC3775] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6," RFC 3344 June 2004.

[RFC4271] Rekhter, Y., Li, T., Hares, S., "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, January 2006.

[RFC4423] Moskowitz, R., Nikander, P., "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

[Sig1998] Signore, T., Girard, M., "The Aeronautical Telecommunication Network (ATN)," IEEE 0-7803-4902-4/98/1998.

[Sol2006] Soliman, H., Montavont, N., Fikouras, N., Kuladinithi, "Flow Bindings in Mobile IPv6," draft-soliman-monami6-flow-binding-01.txt, work in progress, expires December 2006.

[Wak2006] Wakikawa, R., Nagami, K., "Multiple Care-of Addresses Registration," draft-ietf-monami6-multiplecoa-00.txt, work in progress, expires December 2006.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-04-2008	Technical Memorandum	

4. TITLE AND SUBTITLE
Problems With Deployment of Multi-Domained, Multi-Homed Mobile Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ivancic, William, D.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
WBS 430728.02.04.02.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135-3191

8. PERFORMING ORGANIZATION REPORT NUMBER
E-16286

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORS ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER
NASA/TM-2008-215065

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category: 04
Available electronically at http://gltrs.grc.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 301-621-0390

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document describes numerous problems associated with deployment of multi-homed mobile platforms consisting of multiple networks and traversing large geographical areas. The purpose of this document is to provide insight to real-world deployment issues and provide information to groups that are addressing many issues related to multi-homing, policy-base routing, route optimization and mobile security - particularly those groups within the Internet Engineering Task Force.

15. SUBJECT TERMS
Communication; Networking security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email:help@sti.nasa.gov)
U	U	U	UU	13	19b. TELEPHONE NUMBER *(include area code)* 301-621-0390