NASA's Proposed Requirements for the Global Aeronautical Network and A Summary of Responses

William D. Ivancic
NASA Glenn Research Center
wivancic@grc.nasa.gov

***Abstract*—In October, 2003, NASA embarked on the ACAST project (Advanced CNS Architectures and System Technologies) to perform research and development on selected communications, navigation and surveillance (CNS) technologies to enhance the performance of the National Airspace System (NAS). The Networking Research Group of NASA's ACAST project, in order to ensure global interoperability and deployment, formulated their own salient list of requirements. Many of these are not necessarily of concern to the FAA, but are a concern to those who have to deploy, operate and pay for these systems. These requirements were submitted to the world's industries, governments, and academic institutions for comments. The results of that request for comments are summarized in this paper.**

***Index Terms*— Network Centric Operations, Internet, Security, Encryption, International Traffic and Arms Regulations, Airspace Systems, Networks, Communication Systems**

I. Introduction

The National Aeronautics and Space Administration (NASA) is performing research and development under the Airspace Systems Program to enable major increases in the capacity, mobility and security of the air transportation system. The Advanced CNS Architectures and Systems Technologies Project (ACAST) within this program is developing technologies intended to improve the performance of the communications, navigation and surveillance infrastructure in support of the program's goals. In 2004, NASA initiated the Secure Aircraft System for Information Flow (SASIF) project, an element of the Aviation Safety Program (AvSP). SASIF is concerned with hardening the radio data links and network communications, mainly directed at hostile act intervention and protection.

NASA is working with other U.S. government agencies including Department of Defense, Department of Homeland Security, Department of Transportation, and the Federal Aviation Administration to define concepts and requirements for transformation of the National Airspace System required to enable a 3 times growth in system capacity. A key concept of this transformation is the development of network-centric information systems which includes the airborne elements.

This work is jointly sponsored by the NASA's Airspace Systems and Aviation Safety Programs.

The NASA Glenn Networking Research Group (NRG) on behalf of the ACAST and SASIF projects has formulated a list of requirements to ensure global interoperability and deployment. Here, global implies interoperability or all elements including network security whereas deployment implies affordability and readily available technologies (i.e. technologies that will be available in the next few years).

The NRG wished to obtain input from multiple sources regarding these salient requirements: (1) as a sanity check; (2) to ensure we did not overlook something of major importance; and (3) to improve upon and refine these requirements.

II. Strategy for Obtaining Input

NASA, as a government agency, has to be very careful not to show favoritism or even give the appearance of favoritism toward private or commercial entities. In addition, the NRG wanted to obtain input from as many sources as possible and as many different types of sources. In particular we were interested in input from non-aeronautics groups as well as from the aeronautics community in hopes of broadening the aerospace communities' horizons. (e.g. WorldCom, Sprint, DoCoMo, Samsung, Panasonic, Sony, Ford, Toyota, US DoD, Eurocontrol, China, Korea, Wide Project, IPv6 Summit, IPv6 Forum, 3GPP, British Telecom, T-Mobile, Microsoft, Cisco, Intel, etc.).

Thus, in order to be completely open in requesting input and ensured fairness, on February 8, 2005, NASA released a formal request for information (NNC05ZVI011L) seeking comments on these requirements with the intent to encourage open response that could be shared globally. This formal RFI expired on March 28, 2005. They are available at the following URL: http://roland.grc.nasa.gov/~ivancic/RFI/responses/responses.html.

As many of the various groups we wished to reach do not necessarily monitor the federal business advertisements, additional emails and solicitations for input were sent to this audience. Links to the request for comments (RFC) were posted on a number of Web sites such as: the Association for Enterprise Integration (AFEI) the Airborne Internet, ICNS Conference, IST IPv6 Clusters web sites and the 6sense IPv6 newsletter [1-5]. A request to respond was also sent to the IP

Security, Networks in Motion, Mobile IPv4 and Mobile-IPv6 working groups.

As of May 2, 2005, NASA is in the process of sending a letter to a number of National and International airlines requesting comment. Ultimately, the airlines pay the bill – they purchase the planes, pay for communication systems, pay for maintenance and pay for security requirements mandated by government agencies. Thus, NASA would greatly appreciate their input. NASA would also like to hear from the automotive industry as there is much synergy between the airline and automotive transportation industries with the automotive industry providing the necessary volume to drive down system costs.

Although the formal RFI has closed, the NRG is still extremely interested in receiving comments regarding these salient requirements and input regarding future requirements pertaining to network-centric operations for both airspace system user operations and air traffic management. Comments are being sought from those directly involved in aeronautics, as well as telecommunication, communication, computer, information assurance providers and electronic appliance manufacturers. We believe those outside the traditional aeronautics community have expertise and insight that is directly applicable to network centric operations.

III. Request for Comment

The following two sections contain the salient requirement and design concepts from which the Global Airspace System will be based. *Although many of these requirements and design concepts may appear obvious, general, or somewhat simplistic, the implications of changes to network operations and policy are significant!*

A. Global Airspace System Requirements:

- Must be value added
  - Cannot add cost without a return on investment that meets or exceeds those costs.
- Must operate over Global Airspace System, not just National Airspace System
- Must be interoperable throughout the World (not just US friendly nations)
- Must be capable of utilizing whatever links become available – link independent
  - Must be able to perform critical Air Traffic Management (ATM) functions over low-bandwidth links
- Must use the same basic security mechanisms for Air Mobile and Ground Infrastructure (surface, terminal, en router, oceanic and space)
  - Critical ATM messages must be authenticated.
  - Must be capable of encryption when deemed necessary
  - Security mechanisms must be usable over entire Global network
    - Must not violate International Traffic in Arms Regulations (ITAR)
- Must operate across networks owned and operated by various entities
  - Must be able to share network infrastructure
- Must use same technology (i.e. core networking hardware and protocols) for aeronautics as will be used by other industries (e.g. automotive, medical, banking, etc).
- Must enable sharing of information with proper security, authentication, and authorization
  - Situational Awareness
  - Passenger Lists
  - Aircraft Maintenance
- Same network must accommodate commercial, military and general aviation.

B. Design Concepts:

- Must be IPv6 based.
- Must be capable of a prioritized mixing of traffic over a single RF link (e.g. ATM, maintenance, onboard security, weather and entertainment).
- Must utilize IPsec-based security with Security Associations (SAs) bound to permanent host identities (e.g. certificates) and not ephemeral host locators (e.g. IP addresses).
- Must be capable of accommodating mobile networks.
- Must be capable of multicasting
- Must be scalable to tens of thousands of aircraft

IV. Responses

As of April 2005, NASA had received 8 responses from companies and two individual responses from personnel working for United States government agencies. These responses have ranged from simply providing information on the company and product literature to addressing each requirement on a point-by-point basis. The public responses have been placed on an open Web server whereas the "for government use only" responses have added restrictions to allow only specific United States government agencies to view those documents. Add responders have been encouraged to make as much of their response as possible open to the general public. Responses are available at the following URL:
http://roland.grc.nasa.gov/~ivancic/RFI/responses/responses.html

Responses have mainly come from both the aerospace industry and the information technology industries. The NRG is somewhat disappointed that we have yet to get any responses from the electronics industry, the mobile phone communications industry or the automotive industry. This was not surprising, just disappointing. The NRG understands that it takes significant time and money to respond to such a request and that without an identifiable return on investment (ROI) for the company, it is difficult to justify participation – particularly since an open response, to some extent, exposes the business plans of that company.

The NRG will continue to encourage participation from these industries. In addition, we will continue to educate companies as to the potential ROI available from the development and deployment of the Global Airspace System.

V. Monitoring Organizations

A quick monitoring of the system logs was performed to ensure the "for government use only" input was properly protected and not able to be accessed by inappropriate organizations or individuals. During this audit we noted that the material is being viewed by a variety of government and private organizations throughout the world. In addition, over and order of magnitude of organizations have looked at the responses versus providing input.

VI. Results

In general, the responses supported both the general requirements and the design concepts. The process as a whole has been quite useful in sanity-checking our goals and highlighting research areas that still need to be worked.

There is definitely room for debate on the use of gateways for legacy systems. Responders that currently support existing systems and architectures tended to be more inclined to utilize gateways and perceived operations continuing over existing VHF and satellite links. Others considered new capabilities that would become available in the future with the deployment of new broadband link technologies. Overall consensus agreed to six major points:

1) Positive Return on Investment (ROI) is critical.
2) IPv6 is the way to go – virtually everyone agrees on this point.
3) Links should be shared, and the system should be provider-independent. This makes QoS a requirement.
4) A common global security structure must be developed and IPsec is probably the best choice. Some work still needs to be done cleaning up IPsec regarding multicast, envisioning the certificate architecture, and figuring out how exactly to do QoS with encryption.
5) The system must be able to share network infrastructure.
6) The system must be extensible to meet future needs.

A. Return on Investment (ROI)

The system must provide measurable positive ROI. This requirement should apply to all stakeholders in the system including Air Traffic Services (ATS) providers (civil aviation authorities) and ATS users (airlines, military users, and general aviation). Lessons learned from the experimental deployment and recent cancellation of Controller-Pilot Data Link Communications (CPDLC) in the Miami Air Route Traffic Control Center (ARTCC) illustrate that ground and air users cannot and will not invest in new systems for the sake of advancing technology. These organizations must obtain a measurable return on investment.

B. IPv6

IPv6 is being mandated by the United States Department of Defense [6] and will soon be adopted by other US government agencies such as the Department of Homeland Defense. In order to be interoperable with these agencies, deployment of IPv6 is a necessity.

There are significant areas that need to be addressed regarding IPv6 – particularly when considering security and mobility. IPv6 provides many new tools within its structure and has features for standardized deployment of IPsec – in particular authentication and encryption[1].

C. Shared Links

Link independence is an important requirement that facilitates globalization and supports positive ROI over the long run. Thus, applications should be developed so they are link independent. Link independence allows for the system performance and capacity to be improved when new link technologies become available without changing each of the implemented applications. Whether these links should be over an open systems is debatable. Thus, to what degree these links can be provider independent is open to discussion. The major issue being quality of service (QoS) controls more than security issues.

D. Common Global Security Structure

ITAR and other export laws will need to be well understood and considered throughout the planning and implementation of the Global Aeronautical Network. Within the U.S. there are numerous regulations regarding the export of technology from a variety of agencies (for example, U.S. Department of Commerce, Bureau of Industry and Security and Export Administration Regulations). Similar regulations exist in developed nations throughout the world.

IPv6 is a positive step toward this goal as IPv6 inherently supports IPsec for authentication and encryption.

Use of IPsec for mobile networks and hosts or for IPv6 with dynamic addressing is currently difficult because IPsec security policies have traditionally been associated with point-to-point addressing. If the source addresses are unknown or changing, it becomes quite difficult to developed scalable security policy databases (SPD). Using a certificate-based system will enable the use of the networked objects certified identity for the SPD in place of statically defined IPv6 addresses. This also enables the use of public private key pairs with certificates to establish trust and identity. Encryption will use these keys. The keys simplify the security policy database and are independent of the IPv6 addresses. Such certificate-based identity may also be useful in enabling use if IPsec for multicast.

In order to be responsive to time-critical authentication and/or encryption, the architecture placement of certificate

[1] IPv6 has a standard way to implement IP Security. However, one does not have to implement IPsec. Note, using IPv6 does not necessarily mean one is deploying security!

servers (key servers) and proper caching of certificates is critical. There simply is not sufficient bandwidth available to ensure high bandwidth connectivity to mobile platforms (e.g. planes, helicopters, unmanned aircraft and vehicles on the tarmac) with currently deployed aeronautical link technologies.

E. Sharing Network Infrastructure

Sharing of network infrastructure is desirable. However, over what types of networks is an open issue. Current systems are generally the property of Governments, service providers or consortia. The basic reason is to control QoS. Thus, if one wishes to send ATM traffic across the general Internet, there is much work that needs to be done to ensure that QoS requirements of critical traffic can be met or that critical ATM traffic can be restricted to specific networks. The former potentially enables high ROI. The latter is somewhat business as usual.

F. Flexible and Extensible

- The design of the Global Aeronautical Network must include strategies for incorporation of legacy and future technologies. Gateways can be effective for legacy network integration.
- The ability to operate across networks owned and operated by various entities will allow system capacity to be increased simply by acquiring additional bandwidth from the most economically advantageous source.
- Use of the same core networking technologies as other industries allow the Global Airspace System (GAS) to benefit form the steady flow of technologies precipitated by those industries.

VII. Policy Implications

One motivation for generating the generic specifications and design criteria was to educate the policy decision makers of the implications that policy has on the ability to implement and deploy a network centric operations system for the GAS.

IPv6 is a very powerful protocol. Existing policies regarding architecture and security can quickly limit the tools and features available in IPv6. For example, IPv6 can enable peer-to-peer secure networking *only if policy so allows*.

Use of the best link available implies that all communications is networked. That is, the current stove-piped architecture is obsolete. For example, pilot-to-controller communication can take place over the best available link. That means the controller operations are networked. There is no longer just point-to-point communications through one radio system and one known path. Rather, that point-to-point communication can occur over any path and RF link and that path and/or RF link may change in the middle of communications.

Operation across networks owned and operated by various entities requires a change in policy. Currently ATM information is sent over its own point-to-point links and internal aeronautical network. ATM traffic is not mixed with other traffic, nor does it cross open networks. The latter requires security and QoS to be specifically addressed.

Current policy requires new systems to be “make-before-break” rather than “break-before-make” even though current systems do not operate in this capacity. Such requirements may not allow use of COTS standards and equipment. Also, a “make-before-break” implies the same information being sent over multiple links. The negative effects of doing this are usually uncovered during operations. For example, it is well documented that one should not split a single message flow over multiple paths. The results are often much worse performance than using a single path. Thus, “break-before-make” may result in worse performance, not better performance [7-8].

Current policy requires policy-based routing. How one performs policy-base routing over dynamic RF links is problematic. Also, the need for policy-based routing is highly questionable as the best available link may not be known in advance? One may force ATM over a link that appears to be operational, but is not (e.g. the interface is active, but no protocols are running over the link).

The policy makers need to understand what the real QoS requirements are. Those requirements should consider the application and the phase of navigation operations (e.g. surface area, enroute, oceanic, etcetera.).

VIII. Areas Requiring Further Investigation and Research

Quality-of-Service over various links and shared networks requires extensive investigation. Prioritization of traffic is relatively easy to do with today’s technology. However, even though that traffic has high priority, this does not mean it will meet the current requirements over all RF links or routes – particularly if some of that traffic is sent over the open Internet. For example, satellite links using higher bands do not have much of a bandwidth constraint, however these add additional delays, which may be unacceptable for certain applications such as ATC in terminal airspace. Likewise, use of 3rd generation (3G) cellular technology [9-10] in terminal airspace may be sufficient, but may not provide the connectivity enroute. Together, satellite and 3G may provide the majority of the required capability with VHF systems maintained as backup.

Use of mobile networks the air-ground links should be investigated to determine if current and pending technology can meet the reliability and QoS ATM requirements without the use of “make-before-break” techniques or policy-base routing.

Use of mobile networking or ad hoc networking for oceanic operations should be investigated. Satellite links tend to be quite expensive. Use of ad hoc technology has the potential to reduce or perhaps eliminate the need for satellite communications for ATM traffic. This would be particularly beneficial when operating above the Artic Circle. Such techniques may also be useful over the continents.

Security architectures and certificate-based security need investigation to determine the placement of certificate-based servers, the amount of bandwidth needed, what applications need authentication only or encryption only or both and how one implements certificate-based security.

IX. Recommendations

Any departure or modification of a standard is non-standard and will result in very substantial cost increases. In addition, there may be a decrease in reliability due to the low number of users testing and utilizing these modifications. Thus, it is imperative that COTS standards be utilized as is or influenced at the standards making bodies rather than modified for aeronautic needs.

An iterative Government – industry dialog through the appropriate working groups and forums will ensure the best and most current technical information is available to make informed decisions.

One needs to consider the entire system and how it operates when considering if reliability and QoS requirements are being met.

Many of the questions regarding QoS can only truly be answered by building out a portion of the system. Modeling and simulation will only go so far.

X. Conclusions

An observation worth noting: Those companies currently working in the ATM arena appeared to have a more conservative approach than those from other industries with regard to network centric operations, use of open networks, and the type and variety of links that may be exploited. There are a number of possible reasons for this – some which are listed below:

- They understand the problem better.
- They have to work daily with the FAA and other international aeronautical standards organizations. Politics may play a role here.
- They are producers of legacy equipment. As such, it is in that organizations best financial interest to maintain the viability of that equipment for as long as possible.
- They do not understand some of the new technologies as well as others.

In general, the responses received to the RFC supported the salient requirements and design criteria. The major difference in responses was related to how well a system may be able to meet reliability and QoS criteria when operating over "the best available link" where that link consisted of both a variety of RF links and a variety of network both owned and operated by various entities. Furthermore, there was full consensus that IPv6 should be used in the backbone, but some contention on its use over air-ground links.

The underlying questions that will ultimately drive the design and implementation are:

- What compromises are acceptable between QoS and control of the network?
- What is acceptable QoS?
- How does one pay for the system?

Acknowledgments

The NRG group thanks all the companies and individuals who responded (or will respond) to our request for comment. We know it takes considerable time and effort to supply such input.

The author thanks all the members of NASA's network research group who provided input to the generation of the RFC as well as discussion regarding the results. Many of the observations and points made during those discussions have found their way into this paper.

References

[1] www.ist-ipv6.org, May 2005
[2] www.usipv6.com, May 2005
[3] www.afei.org, May 2005
[4] www.airborneinternet.com/Intro.htm, May 2005
[5] spacecom.grc.nasa.gov/icnsconf/, May 2005
[6] DoD CIO Memo - Internet Protocol Version 6 (IPv6) Interim Transition Guidance dtd Sep 29, 2003 http://ipv6.disa.mil/docs/stenbit-ipv6-guidance-20030929.pdf
[7] C. Ma, and K. Leung: "Improving TCP Reordering Robustness in Multipath Networks," 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) 0742-1303/04
[8] SITA: "ACARS Duplicates," Datalink Users Forum, San Francisco, CA, February 2005 http://www.arinc.com/aeec/projects/users_forum/presentations/california_05/03_2_SITA_DLUF.pdf
[9] http://www.3gpp.org/Default.htm, May 2005
[10] http://www.g3cars.com/, May 2005