Comments

Subject

Research & Development Priorities
For
Desirable Features of a

Nationwide Public Safety Broadband Network

Offerer
Science Applications International Corporation (SAIC):
A U.S. Owned Company

Technical POC	Administrative POC
Ken Carlberg, Ph.D.	Sarah Campbell
Principal Systems Engineer	Senior Contracts Manager
SAIC	SAIC
1710 SAIC Drive, McLean, VA 22102	1710 SAIC Drive, McLean, VA 22102
Tel: 703.676.7452	Tel: 703.676.6512
Fax: 703.676.5557	Fax: 703.676.7378
Email: Kenneth.G.Carlberg@saic.com	Email: Sarah.J.Campbell@saic.com

This response to a Request for Information (RFI) includes data that shall not be disclosed outside the government and shall not be duplicated, used, or disclosed, in whole or in part, for any purpose other than to evaluate this response. If, however, a contract is awarded to this offerer as a result of, or in connection with, the submission of these data, the government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to these restrictions are contained in all sheets. In addition, the information contained herein may include technical data, the export of which is restricted by the U.S. Arms Export Control Act (AECA) (Title 22, U.S.C. Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401, et seq.).

Statement

This document presents a series of comments in response to the notice and Request For Information (RFI) issued Monday, September 12, 2011 by the National Institute of Standards and Technology [Docket No.: 110727437-1433-01]

General Comments

1. There is a significant monetary cost in adding prioritization support to a network. Existing systems such as Wireless Priority Service (WPS) and the Government Emergency Telecommunications Service (GETS) are prime examples of the cost, management, and form of prioritization service made available by carriers on their existing commercial infrastructures. These systems also reflect the constraints placed on users and the system when prioritization is realized as a network-centric architecture.
2. Prioritization is typically realized in the form of explicit signaling used to distinguish and prioritize one form of communication (e.g., voice versus email) and a particular session from others. One perspective that tends to be ignored is that of preferential treatment of communication. As an example, traffic engineering that can segment various types of traffic can provide greater resiliency and QoS even though no signaled prioritization has been invoked.
3. Dedicated government infrastructures provide a measure of managed control that helps facilitate the incorporation of new features, compared to an acquisition process dependent on commercial infrastructure (i.e., carrier, Internet Service Provider) offerings. However, it needs to be noted that the impact of disasters may arbitrarily damage infrastructures. Hence, there may be cases where commercial infrastructures experience less damage and faster restoration than government owned infrastructures.
4. While a need for interoperability is identified in the RFI, there did not appear to be a specific need to provide a seamless gateway service between legacy Land Mobile Radio (LMR) systems and the proposed Nationwide Public Safety Broadband Network. This issue can be particularly acute in cases where existing solutions used to gateway legacy LMR systems is accomplished by proprietary solutions.
5. The RFI does not identify the use the Internet Protocol (IP) as an underlying foundation, in terms of technology or standard, for the infrastructure used to realize a new Nationwide Public Safety Broadband Network. While it is understandable for the government to minimize constraints in any proposed design, a targeted reliance on IP allows researchers, developers, and providers to propose specific ideas and identify gaps that need to be addressed in supporting a nationwide first responder network.
6. Upon review of the 15 operational requirements, one significant omission is the subject of congestion management.

Specific Comments and Recommendations

1. ***Reactions to Congestion for Real-Time Applications.*** Recent work-in-progress within the Internet Engineering Task Force (IETF) standards group has involved adding Explicit Congestion Notification (ECN) for real-time applications like voice and video. Since this effort makes ECN information available to applications, we recommend leading edge development that allows various reactions (even exemption) from congestion notification. This would address some of the Quality of Service operational requirements cited in the RFI. We point the reader to the following link for further

technical documentation of this design: ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-avtcore-ecn-for-rtp-04.txt

2. ***Interoperability with Legacy LMR***. At present, the primary means of providing interoperability between Project 25 (P25) LMR systems is through a proprietary interface known as the Inter-RF Sub-System Interface (ISSI). While the ISSI standard has been available for other vendors to build from, its control in terms of modifications and releases are under the management of a single commercial enterprise. We recommend the development of an open (intellectual property-free) design to accomplish the goals of the ISSI as well as rely on IP as an underlying gateway infrastructure. This effort would allow mechanisms like IP multicast to map seamlessly with LMR talk groups in such a way as to optimize and minimize resource utilization. We note that this gateway would need to operate and be developed to support several different deployment scenarios.

3. ***Smart Edge Designs***. The success of the Internet is due in part to its architectural goal of allowing hosts (clients and/or servers) to incorporate new features and capabilities without requiring additional capabilities in the transit network. The World Wide Web is the best example of this smart-edge/dumb-core architectural design.

   Experience with WPS and GETS have shown that adding priority or preferential treatment to communications is facilitated by additional capabilities added to the network. However, these systems are representative of the smart-core/dumb-edge design inherent in legacy circuit switched architectures of carriers. We recommend a hybrid architecture that encourages new features in the network while at the same time promoting additional capabilities in the end host (e.g., smart-phones). One such example is listed in item (1) above. Another example could be manifested in Mobile Ad-Hoc Network (MANET) style communications between "local" participants in cases where access network infrastructures have been destroyed by natural or man-made disasters. A third example would be downloading new capabilities from a "cloud" repository as the need or service is required. Item (4) below expands on this example in the context of authentication.

   We also recommend multi-band communication devices that can seamlessly operate over a next generation network dedicated for first responders as well as commercial networks. By relying on smart edge devices operating over a common IP substrate, first responders could achieve a number of their objectives without being constrained to a particular provider or underlying infrastructure.

4. ***Mobile and Temporal Authentication.*** AUTOVON and WPS are classic examples of an end-node based authentication system, where the actual device in use is what is authenticated. Users that access that device have an added capability of invoking prioritized service, but this service does not "travel" with the user to other devices. GETS is an example of a mobile priority service in that the authentication is achieved with a PIN entered by a user on any phone. We recommend applying this mobile authentication model to any nationwide next generation system established for first responders. We also recommend the inclusion of a temporal characteristic to the authentication so that it can expire after a certain period of time. This added feature addresses the scenario where a user abandons or loses a device that has features (e.g., prioritization) that should not be available to other non-authorized users. Put another way, one needs to add assurance that the service always travels with the user and not simply the device.

Use or disclosure of information is subject to the restriction on the title page of this response