# Open Infrastructure for a Nationwide Emergency Services Network

**Mark Gaynor**
Boston University
mgaynor@bu.edu

**Alan Pearce**
Information Age Economics
IAEpearce@aol.com

**Scott Brander**
Harvard University
sob@harvard.edu

## ABSTRACT

The paper suggests and supports a public policy in which the Federal Communications Commission should seize a unique opportunity to resolve some of the nation's critical communications problems in times of crises with the allocation of a portion of the spectrum at 700 MHz for the deployment of a nationwide interoperable emergency broadband wireless network built by a public-private partnership. It then presents a convincing theoretical model that advocates that an open and/or neutral, as opposed to a closed, network will add greater efficiency, greater choice, while advancing public safety along with the deployment of new and valuable technologies, applications and services.

### Keywords

EMS Network, emergency services, 700MHz spectrum, open network architecture.

## INTRODUCTION

Traditional economic markets cannot always meet all of the needs of society [Pearce, 2006]. Public Safety is one example where business and government must cooperate for the overall benefit of society. With correct public policy and open infrastructures, business can thrive while society gains. Because of new threats to society, along with an apparent increase in the number of so-called natural disasters, there is need for new thinking and new solutions in order to deal with these emergencies. The 2008 Federal Communications Commission (FCC) auction of the nationwide D band [FCC, 2007] presents a unique opportunity to resolve some of the nation's communications problems in times of crises.

This article proposes that an infrastructure based on open standards to be built by a public/private partnership would best serve the needs of the Nationwide Emergency Services Network (NESN). Our proposed infrastructure will allow distributed management to promote innovation leading to the introduction of new devices, applications, and services, along with centralized control for nationwide crisis management. In the proposed architecture local entities, e.g., first responders (ambulance, fire and police), are able to develop and deploy emergency services with applications and services that they urgently need that are not currently available, often resulting in unnecessary loss of life and property. Devices manufactured by any vendor should be able to interoperate on this "open" NESN. An "open" NESN will encourage the promotion of innovation and provide economic opportunities for a wide variety of device manufacturers, service providers, and application developers, while promoting greater public safety by enabling more effective and efficient communications at lower costs, while also saving and preserving life and property. We briefly present and discuss a model that in a future version of this paper will be used to prove theoretically that openness in application, services, and devices are critical to maximize the benefits of any Nationwide Emergency Services Network (NESN).

Public safety mobile communications networks in the United States are in dire straits. More than six years after the 9/11 terrorist attacks on New York City, Washington, D.C., and Pennsylvania, the public safety community still lacks the resources to build a robust and interoperable nationwide network to serve public safety and national law enforcement agencies [Lipton, 2006, Pearce, 2006]. First responders lack the basic voice and data communications services that they need to confront terrorism, natural disasters, chemical spills, and other emergencies that threaten life and property and cost the nation multiple billions of dollars annually.

One example of local emerging interoperability of emergency networks is the Capital Wireless Information Network (CapWIN) organization [Capwin 2007]. Capwin was created in the Washington area because communication networks of fire, police, and other emergency services were not interoperable between departments, and were not interoperable across municipal boundaries. Police from the DC area did not have effective communications with their counterparts in Virginia and Maryland. By building a local, interoperable network Capwin will enable communication between organizations across geographic areas. This idea should be replicated throughout the country.

The D band spectrum at 700 MHz ideally fits the needs of a NESN because this spectrum is nationwide, unencumbered, and has good physical propagation properties. Combined with the FCC proposed regulations concerning network build out and performance parameters the D band could meet the nation's needs for effective communications in critical situations. This spectrum is unique because of the requirements for current users to vacate the spectrum by 2009 and its nationwide coverage. Because of the propagation properties of this spectrum, the infrastructure will be relatively inexpensive to build, and will work with devices behind walls and in buildings. The D block offers a rare opportunity to build a robust and comprehensive NESN network.

## OPENNESS OF NESN

A wireless network can be open to devices, applications, services, and transport. It can also be closed, which means that the network operator or owner determines what devices, applications and services are to be offered and what are rejected. Openness means that any manufacturer can build a device, subject to open technical specifications and standards that can be used by any end user, on any network. Openness in the context of applications and services means that any end users can pick any application or service they desire, and use them over the open network. Finally, openness in the context of transport services means that the transport network service provider must sell bandwidth at a wholesale cost to others that also wish to provide competitive and/or alternative transport services.

Openness can be complex. A transport network provider may require a certification process to use a device, or run an application or service over the network. This certification process may be complex and expensive, which can be a barrier to entry for potentially competitive or emerging companies. Organizations may claim that they support openness, but may take actions that do not promote it. An example is complex document standards. The complexity of some standards makes it to expensive for some organizations to compete effectively.

There is a fine line between applications and services. Voice over Internet Protocol (VoIP) can be both an application and a service. Using Session Initiation Protocol (SIP) two end users can talk over the Internet with a complete end-2-end (described later.) architecture. Only the two end devices know that a voice conversation is occurring. Clearly, this is an application. However, the same protocol, SIP, can be used to create a service where a SIP proxy provides a VoIP service. To a user, the application and service may appear identical.

Google has proposed to the FCC that the C band of the 700MHz spectrum have the following open requirements:

"

- Open applications: consumers should be able to download and utilize any software applications, content, or services they desire;
- Open devices: consumers should be able to utilize a handheld communications device with whatever wireless network they prefer;
- Open services: third parties (resellers) should be able to acquire wireless services from a 700 MHz licensee on a wholesale basis, based on reasonably nondiscriminatory commercial terms; and
- Open networks: third parties (like internet service providers) should be able to interconnect at a technically feasible point in a 700 MHz licensee's wireless network.

" [Google 2007].

## ESN INFRASTRUCTURE

In order to achieve the maximum benefits to society, an NESN must follow at least the first three of Google's recommended openness requirements: open devices; applications; and services. We believe that wholesaling basic transport service would provide a more open and vibrant marketplace, but we do not think that all is lost if wholesaling is not included, as long as the other three openness requirements are present. Openness is designed to create an environment where device manufacturers can innovate with new devices, where application developers have opportunities to discover novel applications, and where successful applications can become services that match the uncertain needs of first responders. This environment is conducive to innovation and must also promote enough management structure to meet the needs of emergency responders in chaotic environments. 9/11 has taught us many lessons, including how traditional communication networks can quickly become overwhelmed with traffic during and after a crisis.

### Standards Based

The Internet has taught us that a rich eco system does develop around open networks built from standards. Under the direction of the Internet Engineering Task Force (IETF), the Internet has become a model of how voluntary standards can build an interoperable infrastructure. In turn, this infrastructure promoted the emergence of many successful ventures for devices, applications, and services. Examples of these successes include devices such as Personal Digital Assistants (PDAs) and Internet enabled cell phones, applications like e-Bay, and Amazon.com, and services such as those offered via VoIP by Vonage, among others.

A degree of centralized control and management will benefit a NESN because of the importance of maintaining a robust network that is not overwhelmed with traffic. Wholesaling transport services on a NESN does not seem to be an absolute requirement in order to create an eco system of vendors, applications developers, and service providers as long as they can use their devices, applications, and services on the NESN, but it would likely increase the number of players.

We agree with the report, "Communications Issues for Emergency Communications Beyond E911" [NRIC focus Group 1D, 2005] that IP should be the underlying standard for the NESN. We also believe that there must be no network-specific functions that would inhibit the ability for any IP-based application to operate fully. This is also in line with the all "IP mantra" for Third Generation (3G) wireless services that most wireless service providers have adopted. The IP protocol has demonstrated the flexibility of an unreliable datagram service for building a vast array of different network applications and services. Using IP will enable the NESN to interoperate with existing IP networks, including the current Internet, and will increase the transport options for the NESN. The use of IP will also mean that NESN deployment can take place in parallel on existing infrastructures and on the infrastructures that will be deployed as a result of the 700 MHz auction, thus maximizing the speed of deployment.

### End-2-end

An end-2-end infrastructure for a NESN is preferred because it has spurred the innovation that underlies the success of the Internet and the World Wide Web and provides many valuable lessons for designers of flexible infrastructures. The end-2-end principle states that networks should provide only the simplest of services [Saltz et al. 1984] [Isen 1998]. The end systems should have responsibility for all applications and any state information required by the application. By providing the basic building blocks, instead of complex network services, the network infrastructure will not constrain future applications. Services with end-2-end architecture, by definition, have a distributed structure because they push complexity to the endpoints of the network. The idea is to keep the network simple, and build any needed complexity into the ends, or edges, of the network. Applications that are end-2-end are generally unknown, or neutral, to the network infrastructure. This means that changes to the network, or permission to add new end-2-end services, are not necessary, because nothing within the network inhibits or constrains a new service. The end-2-end structure is one of increased innovation, and the proof of its validity is the success of the Internet and World Wide Web. The network does need to provide support for some middleware services including authentication and access control. However, the services themselves should be distributed with local entities responsible for their users wherever they are accessing the network.

End-2-end also guarantees that services offered by the network infrastructure are as simple as possible. If you try to anticipate the services that applications will need, you are likely to be wrong, and as a result may inhibit new

applications by constraining them with services that do not serve the needs of the public. The IP protocol in the Internet is a good example of this philosophy -- it is simple, only offering the most basic type of network service, i.e., the unreliable datagram service. This simple core protocol has allowed immense innovation at the transport and application layers. Different application modules can utilize the transport protocols that match their needs, yet all of them are built over IP, which has become the glue holding the Internet together. The success of the Internet is partially due to the simplicity of IP, which validates the end-2-end argument.

By pushing applications to the user level with end-2-end applications, much more experimentation is permitted. Since end-2-end applications do not require modification of the network infrastructure or permission to experiment, users can and do innovate by creating new services. Consider the creation of the World Wide Web. Tim Berners-Lee [Berners-Lee 1999] was not a network researcher searching for innovative ways to utilize the Internet. Rather, he was an administrator trying to better serve his users. He developed the Web to allow the scientists in his organization to share information across diverse computers and networks. It just so happened that his solution, the Web, met many other user needs far better than anything else at the time. This illustrates one powerful attribute of the end-2-end argument - you never know who will think of the next great idea and with end-2-end services, it could be anybody.

Just as end-2-end argument promoted innovation in the Internet, the value of open infrastructure is greatest when uncertainty is high and users are able to experiment with new devices, applications, and services. Sometimes, as Hippel [Hippel, 1998] shows, users are best suited to solve their own problems and end-2-end infrastructure promotes user innovation.

#### Modified End-2-end

We believe in a modified end-2-end structure for the NEMS. It is important to promote innovation with devices, applications, and services while maintaining the ability to dictate what is used when on the network when. In the Internet anybody can try anything, for example we can try to launch a distributed denial of service attack on any user we desire. Clearly this is not desirable on the NEMS. This boils down to some sort of admissions and authorization control systems to determine who can do what, and when.

Given that we believe the NESN must be based on open standards, vendors can build devices and develop applications and services. However, they should not be able to deploy these new devices/applications/services without explicit permission from the organizations that use the NESN. The combination of end-2-end thinking and admission control should serve society best because it will promote innovation while being able to deliver a network that can meet the stringent requirements of an NESN.

#### Management Structure

Wireless networks can have either a centralized infrastructure, similar to traditional cellular networks, or a more distributed architecture, such as the emerging collection of wi-fi networks. Centralized networks allow better coordination, but do not promote innovation [Gaynor and Bradner 2003]. We prefer the idea of one of our informal reviewers, KC Chaffy at The University of San Diego, who suggested that a portion of the D band be given to local communities to allow experimentation with different wireless infrastructures. She would also like to see infrastructure enabling traffic measurement while protecting user privacy. We welcome both ideas since they promote innovation via experimentation and market selection, and encourage the collection of data to aid network researchers.

#### Priority Service with Admission Control

For effective emergency services, the NESN must support several types of priority services that include prioritization of communications and dynamic admission control. The NESN will carry data, voice, and video traffic from heterogeneous sources. Voice and Video traffic require low latency. Communications for command and control from emergency managers needs priority over less critical information. At the very least we recommend a best effort classification for non-emergency traffic, priority classification for normal emergency communications, highest priority for management emergency traffic, and a low latency category for time sensitive data such as voice and video.

General Internet traffic prioritization has two main favors: a coarse-grained packet classification strategy called differentiated services described in RFC 2475 and RFC 3260 [Blake et al. 1998] [Grossman 2002] and fine-grained

session level reservation methodology called integrated services discussed in RFC 2205 and 4495 [Braden et al.] oriented protocols. We recommend packet level QoS such as diff-serv, which scales well and is robust because there is no per-flow meta-data within the network infrastructure. Diff-serv offers best effort, expedited forwarding behavior for delay sensitive traffic, and up to 12 classes of Assured Forwarding. The scalability and robustness of class based priority offered by the diff-serv architecture is reasonable for the NESN.

The Defense Information Systems Agency (DISA) within the DOD has proposed a "service" architecture for military telephone services, Assured Service [Baker and Polk 2004]. Multi-Level Precedence and Preemption (MLPP) [American 1992] defines a dynamic protocol to assure that the most important calls preempt less critical communications. Multi-Level Expedited Forwarding is a partial solution to MLPP but needs a dynamic admission protocol to begin to satisfy the MLPP requirements [Baker and Polk 2004]. A proposed solution that has both call admission control with packet priority and preemption is discussed in an IETF Internet draft [Baker and Polk 2006]. While current Internet protocols may not fully meet MLPP, they clearly can evolve to meet the communication needs of the NESN.

## VALUE OF AN OPEN ESN

There are ways to value open versus closed architecture. One model that we will discuss in an extended version of this paper is based on basic probability and statistical theory [Baldwin and Clark 1999] [Gaynor 2001 & 2003] [Gaynor and Bradner 2001, 2004, and 2008] along with several assumptions about users, device manufactures, application developers and service providers. It could be used illustrates analytically how market uncertainty affects the value to EMS organizations (i.e. the users) of a NEMS network. The model would predict that when uncertainty is high in the context of what devices, applications, and services emergency organizations will find valuable then an open network has greater overall value than a closed network. The greater the uncertainty and the more choices users have the greater the value of openness

## CONCLUSION

The architecture and the beginnings of a theoretical model outlined in this paper demonstrate that the risk is worth taking to demand openness in any NEMS. Namely that an open beats a closed network in terms of customer service, satisfaction, efficiency, cost, and the development and deployment of new technologies, applications and services. Furthermore, since there is a dire need for the creation of a government mandated nationwide, interoperable broadband wireless network for use of the public safety and national law enforcement agencies, this vehicle, if launched via FCC policy, could be used as a low risk experiment to test the validity of this theoretical model.

## REFERENCES

1. American National Standards Institute, "Telecommunications, Integrated Services Digital Network (ISDN) Multi-Level Precedence and Preemption (MLPP) Service Capability", ANSI T1.619-1992 (R1999), 1992.
2. Baker, F., and Polk J., Implementing MLPP for Voice and Video in the Internet Protocol Suite, IETF 2004.
3. Baker, F., and Polk J., MLEF without Capacity Admission Does Not Satisfy MLPP Requirements, IETF 2004.
4. Baker, F., and Polk J., Implementing an Emergency Telecommunications Service for Real Time Services in the Internet Protocol Suite, IETF May. 2006 (RFC 4542).
5. Baldwin, C. and Clark, K. (1999). Design Rules: The Power of Modularity. Cambridge, MA: MIT Press.
6. Berners-Lee, T., Weaving the Web, Harper, 1999.
7. Black, S, Black, D, Carlson M, Davies, E, Wang Z and Weiss, W, An Architecture for Differentiated Services, IETF Dec. 1998 (RFC2475).
8. Braden, R, Zhang, L, Berson S, Herzog, S and Jamin S, Resource Reservation Protocol (RSVP), IETF Sept 1997 (RFC 2205).
9. CAPWIN http://www.capwin.org/.
10. Grossman, D. New Terminology and Clarifications for Diffserv, IETF April 2002.

11. FCC, http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73, 2007.
12. Focus Group 1D, Communication Issues for Emergency Communications Beyond E911, Final report, Dec 2005.
13. Gaynor, M. (2001). The effect of market uncertainty on the management structure of network- based services. Ph.D. Thesis, Harvard University.
14. Gaynor, M. and Bradner, S. Using Real Options to Value Modularity in Standards. (2001) Knowledge Technology and Policy, Special on IT Standardization, 14:2.*
15. Gaynor, M., Network Service Investment Guild: Maximizing ROI in uncertainty markets, Wiley, 2003.
16. Gaynor, M., Bradner, S. A Real Options Metric to Evaluate Network , Protocol, and Service Architecture, Computer Communication Review(CCR), Oct 2004
17. Gaynor, M., Bradner, S. A Statistical Model to Value Network Neutrality , Media Law & Policy, New York Law School, Accepted March 2008.
18. Google, http://googlepublicpolicy.blogspot.com/2007/07/promise-of-open-platforms-in-upcoming.html, 2007
19. Hipple, E. Economics of Product Development by User: The Impact of Sticky Local Information, Management Science 44(5), 1998.
20. Isenberg, David S., "The Dawn of the Stupid Network," ACM Networker 2.1, Feb/March 1998 pp 24-31.
21. Lipton, Eric, The Katrina Year: The Next Emergency: Despite Steps, Disaster Planning Still Shows Gaps, N.Y.TIMES, Aug. 26, 2006, at A1.
22. Pearce, Alan, "An Analysis of the Public Safety & Homeland Security Benefits of an Interoperable Nationwide Emergency Communications Network at 700 MHz Built by a Public-Private Partnership," Media Law & Policy Journal, New York Law School, Vol. 16, No. 1, 2006, pp. 41-61.
23. Pierce, M and Choi, D., Architecture for Assured Service Capabilities in Voice over IP, IETF Internet draft, Jan 2004.
24. Pierce, M and Choi, D., Requirements for Assured Service Capabilities in Voice over IP, IETF Internet draft, Jan 2004.
25. Saltzer, J, and Reed, and Clark, D. 1984., "End-To-End Arguments in System Design.," ACM Transactions in Computer Systems 2, 4 , Nov: 1984 p 277–-288.