Brian Sandoval
Governor

Chris Perry
Director

Christopher B. Smith
Chief

Division of Emergency Management
Homeland Security
2478 Fairview Drive
Carson City, Nevada 89701
Telephone (775) 687-0300 • Fax (775) 687-0322 • http://dem.state.nv.us/

LTE Broadband and Public Safety

Overview

Long Term Evolution (LTE) is the current technical standard for cellular-style wireless broadband voice and data communications. Commercial "smartphone" technology, with software applications, messaging, and voice communications anywhere, anytime, is the model for Public Safety LTE. This approach aims to provide effective, interoperable wireless communications at faster speeds with better reliability than other technologies. LTE has been selected for use in the Public Safety "D-Block" 700 Megahertz (MHz) spectrum, as part of the Nationwide Public Safety Broadband Network - NPSBN, or the "FirstNet" program.

LTE is sometimes referred to as "4G" by cellular providers. The underlying technology is essentially the same for commercial and public safety uses. Since creating a totally new, nationwide network for public safety is not possible with projected resources, the NPSBN will emerge as a public-private partnership, including assets from all participants. A large part of the public safety network will be made up of commercial assets. LTE services from carriers are generally adequate for consumer use, but not necessarily physically robust enough for public safety. Other unique public safety requirements are administrative - priority access policies and interoperability agreements.

Differences in technology from existing systems will create a learning curve for users and administrators. Coverage issues, particularly indoors, may be substantial. Equipment will be different than most users are accustomed to. Network systems, particularly interconnecting "backhaul" circuits, will require substantial improvements. Since FirstNet holds the radio licenses for the network, agencies will not "own" their spectrum.

While LTE supports voice communications that is adequate for consumer grade communications, it is not yet feasible at the quality and reliability levels required by Public Safety users. There is no "talk-around" capability with LTE at this time.

Beyond technical capabilities, the evolution of LTE capabilities in Public Safety represents the opportunity and necessity for cooperation between agencies and in the public-private space. Data sharing, privacy, security, and system administration issues are very important considerations. Partnerships and sharing agreements are essential.

Funding is uncertain beyond the initial grant monies available for planning purposes only. Spectrum auctions of former analog television channels are expected – but not guaranteed - to raise several billion dollars towards deployment. Subscriber fees are extremely likely to be required.

Public/Private Partnership

Public Safety has something that commercial wireless providers want: Spectrum. Radio frequency spectrum is the critical resource in our telecommunications-heavy society. The public safety D-Block spectrum is adjacent to the private sector's assigned frequencies for implementing LTE/4G. The private sector is interested in the dual use of the public safety spectrum, since they can increase the number of subscribers served by using the D Block. In exchange for use of the bandwidth for general public use, the carriers' LTE networks could be available on a priority basis for public safety. By integrating both groups' spectrum resources, a more powerful network is possible for all users. Ruthless priority would, of course, be required for public safety.

Partnership with private sector carriers may permit the more efficient provisioning of new and changed devices on the public safety network. Since telecommunications carriers routinely change calling plans, numbers, and features on subscriber devices, they have well-established procedures for doing so. The relatively small number of public safety users added to this system might be practical for the carriers to absorb with little impact, or at leas with less impact than establishing new protocols with FirstNet state organizations.

Players

Well-known communications companies are active in the public safety and commercial LTE market. Equipment manufacturers Alcatel-Lucent, Harris, Johnson, Motorola, and others can provide a variety of goods and engineering services. Nationwide carriers AT&T, Sprint, Verizon, and others have well-established networks and the "vertical real estate" of towers throughout the country. Coverage does not, and likely could not anytime soon, extend to every acre of Nevada. Population centers and transportation corridors are generally well connected. Inter-site backhaul data capacity is generally good.

Public-sector players may include every agency with a tower, with a utility right-of-way, or with any kind of technology asset. Since public safety agencies typically have resilient facilities, often equipped with backup power sources, they are natural partners with each other and the commercial side, especially those who share towers. Voice, data (SCADA, etc.), medical, and even educational users will need to pool resources. Properly managed, incorporating the best of each system can create a better network for all users, without diminishing capacity or security.

Data

With LTE data rates of up to 100 megabits per second (Mb/s) per user, the amount of data being transmitted is dramatically higher than on any previous system. Almost no network infrastructure in place now will be enough to support LTE. A major upgrade to the interconnecting "backhaul" network is required, including the need to bring fiber optic cable or some other "fat pipe" to each site. Nevada currently uses a mix of microwave links, traditional copper wiring, and fiber to achieve backhaul. Systems can only transmit as much data as the lowest bandwidth component of any path supports.

Practical user data rates will vary, depending on signal levels, location, network congestion, and other factors. Not every user will experience the same speeds at all times. For comparison, most 3G cellular data transmission ranges from 100 kilobits per second (kb/s) to 4 Mb/s. A typical home DSL wired internet connection provides 6 Mb/s, with a cable modem connection usually sporting 20-100 Mb/s. Data rates in a properly operating LTE system can be up to 100 Mb/s close to a working tower, but degrade to 768 kb/s (or 0.768 Mb/s), at the edge of coverage.

Many demonstrations of LTE have shown simultaneous web surfing, streaming video, and voice teleconferencing, along with database access, remote desktop operation, and GIS mapping. It is not clear where

this data is to be stored, how it will be archived, indexed, or maintained. Access control and governance are serious issues that are unresolved. The confidential nature of public safety information may intersect with public records and "right to know" laws. Intra-agency, interagency, and private-public understandings will need to be established. Data security and control are serious issues with the LTE network, since it is interconnected and shared between multiple stakeholders and the public. Recommendations from the FirstNet Board may provide some guidance, but the unique conditions in each state and jurisdiction will call for the promulgation of rules and procedures applicable locally.

Voice

LTE technology supports voice communications using the "Voice Over LTE" or VOLTE, standard. While adequate for consumer grade communications, it is widely believed that voice carriage on an IP-based LTE network is not yet feasible at the quality and reliability levels required by Public Safety users. Digital voice technology is evolving, but has some distance to go before it can be widely used for critical communications.

Coverage

From our experience with radio systems, we have learned that power output must be limited to prevent interference to adjacent channels. This affects the coverage footprint of particular sites, especially inside structures and between buildings. LTE will have the same issues. In-building penetration will not be what we are used to with current cellular systems. Existing in-building relays will probably not be useful on an LTE network.

Devices

Subscriber devices for public safety LTE will reflect consumer offerings. Ruggedized smartphones, LTE-equipped laptops and tablets, and add-on "dongles" or adapters for existing devices will doubtless be available. Some units are starting to become available as technology demonstrators.

Laptop-style devices often use the Microsoft Windows operating system, providing continuity of user experience with most applications and environments public safety users now enjoy. For users of these types of devices, an LTE network provides an effective extension of an agency or corporate Local Area Network (LAN), allowing normal business activities to be carried out remotely.

Portable tablet and smartphone devices initially appear to be oriented towards the Android operating system. While many individuals use Android-enabled smartphones for their personal communications, training will be required to familiarize others, and to improve proficiency in the public safety specific applications and techniques that will become available. Applications written for public safety devices may not operate on commercial handsets, and vice-versa, owing to data security requirements.

Public safety smartphones and other devices will be bulkier and more costly than their consumer counterparts. Batteries will be larger, since louder audio alerts, frequent use during extended shifts, and the need for reserve capability will require far more capacity than consumer devices. Ruggedized construction with superior materials and certified performance (such as Mil Spec) will also boost costs. Of course, the relatively niche public safety market will see higher prices than the mass consumer market.

Funding

In mid-2013, federal funds will begin to become available to begin the LTE transition. The auction of spectrum, formerly occupied by analog television stations in the UHF band, is expected to ultimately provide about 7 billion dollars. Initially, however, Congress has authorized $135 million to be divided between the 56 states and

territories. These funds may not be used for construction or equipment purchases; they are to be used to identify assets and determine requirements in each state. Guidance on applying for these grants will be provided in the first quarter of 2013.

Regardless of the auction outcome, it is considered unlikely that 7 billion dollars can successfully be used to create a nationwide public safety network. Additional appropriations are possible. User fees have also been suggested as a means to raise capital and operating resources. Arrangements between the commercial carriers and public safety users may also defray expenses. FirstNet and SoNNet will likely be responsible for the administration of such agreements.

Conclusion

The Nationwide Public Safety Broadband Network will be realized through public-private partnerships creating a vast virtual network of different commercial carriers, supplemented by government-supported capabilities in commercially non-viable areas. Public safety administrators will need to work closely with their partners at all levels to determine effective cooperative arrangements and procedures. Radio communications personnel and information technology staff will need to work more closely than ever, as the line between computers and communications technologies dissolves.

Rather than the technical aspects of the Public Safety Broadband Network, governance and management may well be the bulk of FirstNet's and SoNNet's activity. Data security and access control are substantial issues that need to be addressed.

It will be many years before the NPSBN supplants existing Land Mobile Radio and other services. Many agencies will no doubt retain their own communications infrastructure for a long time. However, convergence is upon us. Devices, systems, and capabilities are evolving quickly. The future just got more interesting.

I gratefully acknowledge the work done by David Fein on the first edition of this document, and the excellent input by Chris Magenheimer and Lester Lewis.

George J. Molnar
Nevada Statewide Interoperability Coordinator
November 2012
GMolnar@dps.state.nv.us